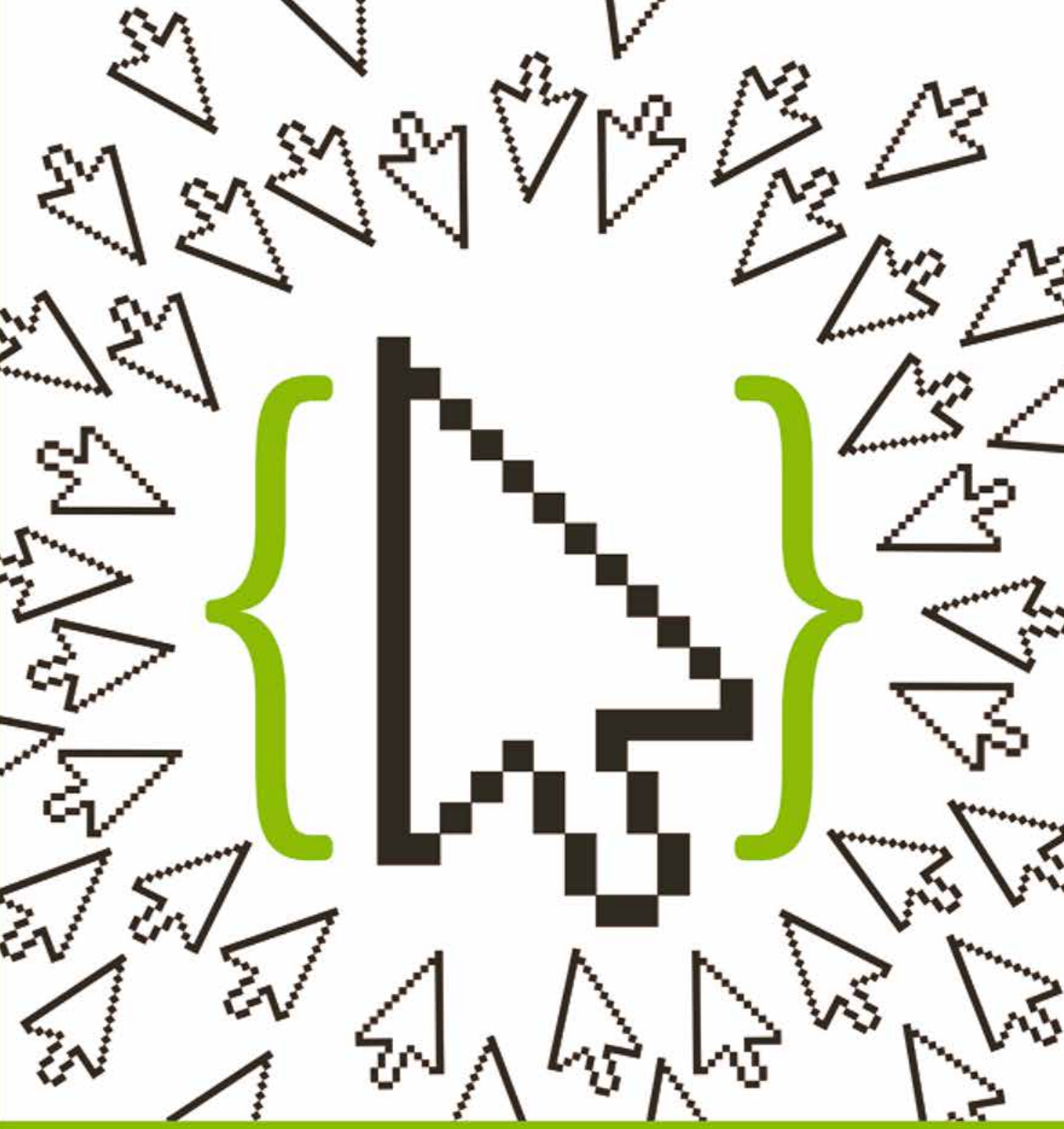


PRIRUČNIK ZA INFORMACIJSKU SIGURNOST I ZAŠTITU PRIVATNOSTI

Uredili: Tena Velki i Krešimir Šolić

Sveučilište Josipa Jurja Strossmayera u Osijeku
FAKULTET ZA ODGOJNE I OBRAZOVNE ZNANOSTI

Sufinancira Europska unija
Instrument za povezivanje Europe

Priručnik za informacijsku sigurnost i zaštitu privatnosti

Uredili
Tena Velki i Krešimir Šolić

Sufinancira Europska unija
Instrument za povezivanje Europe

Uredili:
Tena Velki
Krešimir Šolić

Autori:
Tijana Borovac
Ivan Horvat
Krešimir Nenadić
Ksenija Romstein
Krešimir Šolić
Tena Velki
Marin Vuković

Priručnik za informacijsku sigurnost i zaštitu privatnosti
Osijek, 2018.

Fakultet za odgojne i obrazovne znanosti
Sveučilište Josipa Jurja Strossmayera u Osijeku

Urednici:
izv. prof. dr. sc. Tena Velki
doc. dr. sc. Krešimir Šolić

Recenzenti:
izv. prof. dr. sc. Krešimir Grgić, Fakultet elektrotehnike, računarstva i informacijskih tehnologija, Sveučilište Josipa Jurja Strossmayera u Osijeku
izv. prof. dr. sc. Silvija Ručević, Filozofski fakultet, Sveučilište Josipa Jurja Strossmayera u Osijeku

Lektorica:
izv. prof. dr. sc. Emina Berbić Kolar

Korice:
doc.dr.art. Marko Šošić

Oblikovanje i grafička priprema:
Krešendo, Osijek

Nakladnici:
Fakultet za odgojne i obrazovne znanosti
Sveučilište Josipa Jurja Strossmayera u Osijeku

Naklada:
200 komada

ISBN 978-953-6965-68-7
CIP zapis dostupan je u računalnom katalogu Gradske i sveučilišne knjižnice Osijek pod brojem 141014008.

Objavljivanje ove knjige odobrio je Senat Sveučilišta Josipa Jurja Strossmayera u Osijeku na sjednici 18. prosinca 2018. pod brojem 34/18.

Fakultet za odgojne i obrazovne znanosti
Sveučilište Josipa Jurja Strossmayera u Osijeku

Priručnik za informacijsku sigurnost i zaštitu privatnosti

Osijek, 2018.

Izrada priručnika jedna je od aktivnosti projekta
„Safer Internet Centre Croatia: making Internet a good and safe place“

Ugovor br.: INEA/CEF/ICT/A2015/1153209
Action No: 2015-HR-IA-0013
Nositelj projekta:
Centar za nestalu i zlostavljanu djecu
Partneri:
Fakultet za odgojne i obrazovne znanosti u Osijeku
Grad Osijek
A1 Hrvatska d.o.o.

Priručnik je publiciran uz sufinancijsku podršku programa Department C – Connecting Europe Facility (CEF) od strane Innovation and Networks Executive Agency (INEA) imenovane od strane Europske komisije. Sadržaj ovog priručnika je isključiva odgovornost autora i ne predstavlja nužno stav Europske unije.

Ovaj projekt sufinancira Ured za udruge Vlade RH. Stajališta izražena u ovoj publikaciji isključiva su odgovornost autora priručnika i ne odražavaju nužno stajalište Ureda za udruge Vlade Republike Hrvatske.

VLADA REPUBLIKE HRVATSKE
Ured za udruge

Sufinancira Europska unija
Instrument za povezivanje Europe

Sadržaj

Predgovor

Ideja za pisanje *Priručnika za informacijsku sigurnost i zaštitu privatnosti* nastala je prije više godina tijekom razvoja prvih inačica upitnika o rizičnom ponašanju računalnih korisnika. Urednici su tada, prvi puta spojili znanja iz dvaju različitih područja, informacijske i komunikacijske te bihevioralne znanosti, kako bi se pozabavili pitanjem najslabije karike u lancu informacijske sigurnosti, odnosno ponašanjem računalnoga korisnika. Prvi su rezultati bili poražavajući, pokazujući da su najveći propusti u informacijskoj sigurnosti nastali neprimjerenim ljudskim ponašanjem, te ukazujući na nužnu dodatnu izobrazbu računalnih korisnika iz područja informacijske sigurnosti. Tada se i razvila ideja o pisanju *Priručnika* i pokretanju odgovarajuće sustavne izobrazbe računalnih korisnika.

U sklopu provedbe projekta *Safer Internet Centre Croatia: Making internet a good and safe place*, Agreement Number: INEA/CEF/ICT/A2015/1153209, urednici su uspjeli realizirati ideju i o *Priručniku* i o dodatnoj izobrazbi. Provedeno je veliko nacionalno istraživanje sa svrhom prikupljanja empirijskih podataka o znanju i ponašanju računalnih korisnika. Upravo je ono bilo temelj za pisanje *Priručnika*, a dio rezultata nacionalnoga istraživanja prikazan je u samom *Priručniku. Priručnik* je osnovna literatura za buduće edukacije računalnih korisnika, posebice što u Republici Hrvatskoj nedostaje znanstvene i stručne literature iz ovoga područja.

Štoviše, provedeno nacionalno istraživanje, kao i sama izrada *Priručnika*, potaknuli su stručnjake, prvenstveno iz područja informacijskih i komunikacijskih te bihevioralnih znanosti, da pokrenu i novi poslijediplomski sveučilišni studijski program koji se upravo ciljano bavi ovom problematikom, pitanjima zaštite privatnosti i digitalnih podataka.

Urednici

Tena Velki i Krešimir Šolić

1. UVOD

Pitanje informacijske sigurnosti zabrinjava sve veći broj stručnjaka, iz različitih područja djelatnosti, ali ne samo njih. Mogućnost otuđenja digitalnih podataka, krađa identiteta, bankovnih računa, društvenih profila, itd., zapravo zabrinjava svaku osobu koja se koristi u svome radu, ali i svakodnevnim privatnim aktivnostima internetom, bilo da je to preko osobnih ili prijenosnih računala, pametnih mobitela, igraćih konzola, pametnih televizora ili nekih drugih uređaja koji omogućavaju pristup internetu.

Istraživanja su jasno pokazala kako su informacijsko-komunikacijski stručnjaci nemoćni u zaštiti korisnika različitih informacijskih sustava kada je u pitanju njihovo osobno ponašanje, koje u najvećem broju slučajeva dovodi do proboja informacijske sigurnosti, odnosno otuđenja i krađe digitalnih podatka, kao i njihove zlouporabe. Mnogi su razlozi tome: neznanje, nedovoljno poznavanje informacijskoga sustava koji se koristi ili jednostavno nesmotrenost i neopreznost pri njegovu korištenju.

Svrha ovoga udžbenika je prikazati koji su to najčešći propusti informacijske sigurnosti zabilježeni među računalnim korisnicima, koja su najučestalija i najrizičnija ponašanja računalnih korisnika po pitanju privatnosti i sigurnosti digitalnih podataka, kao i prikazati neke osnovne skupine korisnika sa zajedničkim rizičnim karakteristikama. Cilj nam je na temelju pregleda prethodnih istraživanja, kao i na temelju provedenoga nacionalnog istraživanja, dati neke osnovne savjete i preporuke svim računalnim korisnicima za sigurniji rad u informacijskim sustavima.

Pojavom novih opasnosti na internetu, pojavljuju se novi izazovi za njihovo sprječavanje, inženjeri informacijski tehnologija poboljšavaju postojeće te razvijaju nove tehničke oblike zaštite. Ne postoji potpuna zaštita, a često je upravo korisnik, odnosno ljudski čimbenik, presudan i najslabiji dio sigurnosti informacijskokomunikacijskoga računalnoga sustava. Stoga je neophodno educirati korisnike, te ih sustavno upozoravati na postojeće i nove opasnosti, kako bi ojačali najslabiji dio sigurnosti ovoga sustava, odnosno čovjeka. Svrha ovoga udžbenika je educirati prosječnog korisnika informacijskokomunikacijskih računalnih sustava, bez ulaženja u same tehničke detalje, o zaštiti privatnosti te načinima zaraze podataka zloćudnim kodom, kako se kriptiraju podatci te koji su osnovni načini zaštite digitalnih mreža.

Kako u Republici Hrvatskoj ne postoji sličan udžbenik koji se bavi pitanjima informacijske sigurnosti i zaštite podataka, nadamo se da će ovaj Priručnik poslužiti kao osnovna literatura za buduće edukacije računalnih korisnika.

izv. prof. dr. sc. Tena Velki
doc. dr. sc. Krešimir Šolić

doc. dr. sc. Tijana Borovac
Fakultet za odgojne i obrazovne znanosti Osijek

2. PREGLED ISTRAŽIVANJA O INFORMACIJSKOJ SIGURNOSTI

Sažetak

Ubrzan protok informacija i sve veća dostupnost informacija, kao posljedica digitalnog doba, donijela je za sobom i pitanja koja se tiču sigurnosti na internetu; koliko smo svjesni važnosti sigurnog korištenja interneta, zaštite osobnih podataka, te znamo li uopće kako se zaštiti u slučajevima zlouporabe podataka? U ovome poglavlju dan je pregled istraživanja u svijetu i Republici Hrvatskoj koji nastoji odgovoriti na neka od pitanja vezana za sigurnost na internetu. Poseban je naglasak na istraživanjima i projektima koji su se bavili sigurnošću djece osnovnoškolske i srednjoškolske dobi, ali i studenata i odraslih zaposlenih osoba. Na kraju rada nalazi se pregled organizacija i projekata koji se bave sigurnošću na internetu.

2.1. UVOD

Razvojem digitalnog doba, koje uključuje pojavu društvenih mreža i mobilnih aplikacija (pametni telefoni, društvene mreže, mobilne aplikacije i sl.), ubrzao se protok informacija što je svakako donijelo značajne prilike i koristi današnjem životu, ali istovremeno nove digitalne tehnologije povećale su niz socijalnih i etičkih pitanja. Informacijska i komunikacijska tehnologija (IKT) omogućuje prijenos i uporabu svih vrsta informacija i predstavlja najprodorniju generičku tehnologiju današnjice. Pitanja koja su se otvorila vezana su za sigurnost na internetu uključuju slučajeve zlouporabe IKT-a u obliku neželjenih podataka, krađe podataka, kršenja intelektualnog vlasništva (plagijata i piratstva), delinkvencije, prekomjerne izloženosti online igrama, cyber-*bullyingu*, prijevari, krađi identiteta, pornografiji, trgovini seksom... Prema UNESCO-vom izvješću (2015) slični problemi pojavljuju se u cijelom svijetu i zabrinjavaju, stoga je preporuka za aktivnijim istraživanjima digitalnog građanstva posebno u zemljama u razvoju, kako bi se dobiveni rezultati mogli koristiti u izradi intervencijskih programa koji su prikladni za potrebe svake zemlje. Djeca i mladi su prepoznati kao osobito ranjiva skupina jer često nisu svjesni opasnosti kojima se izlažu kada pristupaju internetu.

Sukladno nastalim promjenama vezano za sigurnost na internetu, a time i zaštitu osobnih podataka u Republici Hrvatskoj, došlo je do donošenja novog propisa koji osigurava ujednačeno i jednoobrazno postupanje u svim državama članicama EU-a po pitanju zaštite osobnih podataka. Agencija za zaštitu osobnih podataka u Republici Hrvatskoj navodi kako će posljedica donošenja novog propisa biti jednostavnija i jednaka zaštitu prava svih pojedinaca u Europskoj uniji. Europski parlament i Vijeće EU-a postigli su dogovor o novim EU pravilima o zaštiti podataka - Uredba o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka (Opća Uredba o zaštiti podataka) - stupila je na snagu 24. svibnja 2016., a primjenjivat će se izravno u svim državama članicama EU-a od 25. svibnja 2018. U kontekstu navedenoga slijedi kako će djeca moći koristiti određene internetske usluge i servise za koje je potrebno dati osobne podatke isključivo uz roditeljski pristanak - dobna granica će biti između 13 i 16 godina.

2.1.1. PREGLED ZNANSTVENIH ISTRAŽIVANJA O SIGURNOSTI NA INTERNETU

Čini se, kako se dobna granica prvog pristupanja interneta spušta diljem Europe. Dob u kojoj se djeca prvi put koriste internetom varira od zemlje do zemlje. Prema Livingston i sur. (2011) prosječna dob prve upotrebe interneta je sedam

godina u Danskoj i Švedskoj, a osam u nekim drugim sjevernim zemljama (Norveška, Finska, Nizozemska i Velika Britanija), kao i u Estoniji. Prosječne dobi su više (10 godina) u Grčkoj, Italiji, Turskoj, Cipru, Danskoj, Austriji i Portugalu. Budući da sve mlađa i mlađa djeca počinju koristiti internet, internetske sigurnosne kampanje i inicijative moraju biti usmjerene i prilagođene mlađim dobnim skupinama, a istodobno održavati postojeće napore vezane za sigurnost starije djece. U onoj mjeri u kojoj su se dosadašnja nastojanja usredotočila na srednje škole više nego li na osnovne škola, sada je potrebno raditi na obrazovanju i usavršavanju nastavnika u osnovnim školama.

Livingston i sur. (2011) su predstavili rezultate međunarodne studije EU Kids Online koja je provedena 2010. godine, u kojoj je sudjelovalo 25 europskih zemalja (Velika Britanija, Grčka, Italija, Španjolska, Slovenija, Finska, Njemačka, Rumunjska,no ne i Republika Hrvatska). U istraživanju je sudjelovalo 25 142 djece u dobi od 9 do 16 godina koja koriste internet, zajedno s jednim od roditelja. Istraživanje je proučavalo ključne online rizike: gledanje pornografije, nasilničko ponašanje, primanje seksualnih poruka, kontakt s ljudima koji im nisu poznati „licem-u-lice", izvanmrežni sastanci s internetskim kontaktima, potencijalno štetni korisnički sadržaji i zlouporaba osobnih podataka. Livingstone i sur. (2011) su u anketi postavili pitanja djeci o tome koliko često su na internetu te kojim uređajima se koriste kako bi mogli pristupiti internetu. Čak 93% djece stare između 9 i 16 godina su *online* barem jednom tjedno (60% su *online* svaki dan ili skoro svaki dan). Većina djece (58%) još uvijek pristupa internetu preko zajedničkog osobnog računala (PC), iako je pristup korištenjem vlastitog računala odmah slijedeći najčešći odgovor (35%). Gotovo trećina djece (32%) pristupa internetu spajajući se preko svojega televizora, a oko trećine to radi preko mobilnog telefona (31%), dok četvrtina pristupa internetu preko igraće konzole (26%). S obzirom da pristup preko računala već dugo prevladava kao najpristupačniji i na prvome mjestu, postalo je jasno kako su posljednjih godina i neki drugi načini pristupanja internetu postali sve rasprostranjeniji. Oko četvrtina djece koristi internet pomoću osobnog prijenosnog računala (24%) ili dijeljenog prijenosnog računala (22%), što odražava rast korištenja prijenosnih računala općenito, i daje sve veći pristup internetu djeci. Osim toga, 12% djece internetu pristupa preko tableta ili prijenosnog uređaja (na primjer, iPod Touch, iPhone ili BlackBerry) (Livingstone, 2011).

U Maleziji, u 2013. godini u školama se provodio program DigiCyberSAFE u sklopu kojega je provedeno istraživanje u kojemu je sudjelovalo 13 945 učenika u dobi od 7 do 19 godina (učenici osnovnih i srednjih škola) u kojemu su iskazali svoje stavove o cyber sigurnosti, prikladnom ponašanju na internetu i sposobnosti zaštite od rizika DiGi (2014). Rezultati studije su bili od ključne važnosti u

razvoju pristupa za unaprjeđenje digitalnog građanstva u Maleziji, kao i izgradnji kapaciteta usmjerenih na nastavnike, savjetnike i roditelje. Iako više od 80% ispitanika smatra online sigurnost važnom, kada se analiziraju rezultati na koji način djeca to čine još uvijek ostaje oko 40% djece koja ne znaju kako se zaštititi na internetu. Usporedbe između dobnih skupina pokazuju da su djeca u dobi od 15 godina ili manje, izloženija riziku od onih u dobi od 16 do 19 godina. Istraživanje je pokazalo da 45% svih školskih učenika koristi nisku razinu sigurnosti na internetu. Unatoč tome, 52% kaže da se osjećaju sigurno na internetu. Još 38% nije svjesno potrebe za višestrukim koracima koji se mogu poduzeti kako bi se zaštitili na internetu DiGi (2014).

Davis i James (2013) suočene s malim brojem istraživanja koja obuhvaćaju stariju djecu osnovnoškolske dobi odlučili su intervjuirati 42 učenika u dobi od 11 do14 godina, u okolici Bostona (Sjedinjene Američke Države) te prikupiti i analizirati njihova razmišljanja o sigurnosti na internetu, pitanju privatnosti na društvenim mrežama te kako se oni nose s tim izazovima. U ovom istraživanju odlučili su se za intervju i kvalitativnu metodologiju kako bi dobili što bolji uvid u razmišljanja učenika. Istraživanje su provodili u prostorima njihovih škola gdje su dva puta intervjuirali svako dijete te na taj način ostavljali više vremena za razgovor i bolje upoznavanje sa svakim sudionikom, pri čemu su ih pitali da podijele s njima svoje osobne definicije o privatnosti te navedu strategije koje koriste za stvaranje privatnosti na mreži. Rezultati ove studije ukazuju na to da učenici cijene privatnost, traže privatnost od stranaca i poznatih osoba, te provode različite strategije kako bi zaštitili svoju privatnost na mreži. Davis i James (2013) navode kako gotovo svi sudionici studije (njih 40, ili 95%) koriste strategiju koja uključuje zadržavanje sadržaja s *online* prostora. Učenici su rekli kako ne objavljuju određene osobne podatke (kao što su njihova puna imena, adrese i telefonski brojevi) na društvenoj mreži, u porukama i sl. Više od jedne trećine sudionika u istraživanju reklo je kako bi zaštitili svoju privatnost na mreži objavljujući neistinite informacije o sebi. Iako je riječ o malom uzorku i kvalitativnoj metodologiji, autorice su željele ukazati na važnost provođenja ovakvih istraživanja za dobivanje što preciznijih i relevantnijih informacija.

Istraživanje u Republici Hrvatskoj pokazalo je kako postoji razlog za zabrinutost zbog rizičnog ponašanja učenika na internetu, bez obzira na spol ili dob učenika. Prema Velki i sur. (2017) dobiveni rezultati istraživanja trebali bi upozoriti državne institucije i nastavnike u školama i potaknuti na razvoj učinkovitijih obrazovnih programa i programa prevencije s ciljem povećanja sigurnoga ponašanja kada se radi o *online* i informacijskoj sigurnosti i zaštiti privatnosti. Cilj je studije bio ispitati problematiku rizičnoga ponašanja računalnih korisnika na srednjoškolskoj populaciji, a autori su podatke prikupljali putem Upitnika znanja

i rizičnog ponašanja korisnika informacijskog sustava (UZPK) prilagođenog za srednjoškolce. Autori su prikupili informacije o rizičnom ponašanju računalnih korisnika i znanju o informacijskoj sigurnosti između 355 učenika iz triju srednjih škola: gimnazija, ekonomska (četverogodišnja srednja škola) i trgovačka škola (trogodišnja srednja škola). Rezultati su pokazali da je postotak učenika srednjih škola koji su otkrili svoju lozinku za pristup sustavu e-pošte puno veći nego li je uobičajeno (77,7%). Učenici srednjih škola bolje su se procjenjivali na subskalama održavanja osobnog računala i uvjerenja da znaju osigurati računalne podatke, no unatoč tome iskazivali su na ponašajnim mjerama niz rizičnih ponašanja vezano uz informacijsku sigurnost (npr. posuđivanje pristupnih podataka - zaporki, nezaštićena komunikacija i/ili komunikacija s nepoznatim osobama putem interneta i sl.). Osim toga, postoji relativno visok postotak učenika koji su bili *cyber-žrtve*, kao i određeni postotak učenika koji su bili *cyber-nasilni* (Velki i sur., 2017).

Uloga digitalnog građanstva u obrazovnom sustavu je pružiti sredstvo koje pomaže učenicima razumjeti kako se tehnologija upotrebljava na siguran i prikladan način. Neke od ključnih vještina koje učenici trebaju za učinkovito kretanje digitalnim svijetom uključuju: pronalaženje pouzdanih informacija putem interneta, otkrivanje sumnjivog sadržaja, svjesnost pravila o privatnosti s prikupljenim informacijama na mreži i iskorištavanja tehnologije koju nude sudjelovanjem na odgovoran način s drugima širom svijeta (Hui i Campbell, 2018). Slično tome, govori i Thierer (2009) koji kaže da sam fokus na sigurnost djece nije dovoljan. Djeca moraju naučiti kako smanjiti rizike, ali i naučiti odgovorno i etično ponašati se u digitalnom svijetu. Osim toga, trebaju razumjeti medijsku pismenost, kako bi mogli kritički razmišljati o sadržajima koje konzumiraju i sve više stvaraju. Stoga, najbolje prakse moraju nastojati osigurati zabavna, obrazovna i sigurna iskustva za djecu.

2.1.1.1. Pregled istraživanja o sigurnosti studenata na internetu

Vještine i sklonosti korištenja informacijsko-komunikacijske tehnologije su rezultat odrastanja u tehnološki zasićenome okruženju u kojemu tehnološke naprave računala, mobiteli, tableti postaju sastavni dio života. Zbog toga se mlađe generacije razlikuju od starijih ne samo po sklonostima i stavovima, već i prema načinu procesuiranja informacija i učenja, pa sve češće se susrećemo s terminima kao što su *cyber djeca*, digitalni urođenici, google generacija… Navedeni pojmovi oblikuju diskurs o mladima i njihovom korištenju računala. Lasić-Lazić, Špiranec, Banek Zorica (2012, str. 126) navode kako se novi diskurs temelji se „na predodžbi o iznimnim vještinama mladih u korištenju tehnologija i pretpostavci da će se one automatizmom uspješno i pozitivno odraziti na procese učenja, no

rezultati istraživanja o informacijskim navikama, interakcijama i načinima procesuiranja informacija pokazuju da se radi o horizontalnim ili površnim interakcijama koje su usmjerene na kvantitetu podataka umjesto na njihovo kvalitetno tumačenje i kritičko razmatranje koji su pretpostavka za dubinsko, smisleno i istinsko učenje." Shodno tome, postavlja se i pitanje sigurnosti jer sadašnji digitalni urođenici su već na fakultetima i ušli su u visokoobrazovni sustav.

Kim (2014) je utvrdio kako su neki studenti svjesni sigurnosnih problema i razumiju da bi trebali biti oprezniji zbog svoje vlastite sigurnosti, ali nisu ustrajni u provođenju sigurnosnih mjera predostrožnosti korištenja interneta. Do navedenih rezultat Kim (2014) je došao istražujući status svijesti o važnosti informacijske sigurnosti među studentima kako bi razvijali učinkovitu edukaciju o važnosti svijesti o sigurnosti uporabe informacija (ISAT). U navedenom istraživanju došli su do rezultata kako studenti razumiju važnost i potrebu za ovakvom vrstom edukacije kao što je ISAT, ali mnogi od njih ne sudjeluju u tome. Teer, Kruck i Kruck (2007) su ispitivali računalnu sigurnost prakse studenata preddiplomskih studija i zaključili su da „studenti ostavljaju svoja osobna računala ranjiva na viruse". Lomo-David, Shannon i Ejimakor (2009) ispitivali su studente (867 studenata različitih smjerova i razina - preddiplomska i diplomska razina studija) o upoznatosti i korištenju sigurnosnih mjera na internetu. Pod sigurnosnim mjerama mislilo se na korištenje jednostavnih zaporki, sofisticiranih zaporki (sastoje se od kombinacije velikih i malih slova, brojeva te znakova), zaporki u privitku e-pošte, svakodnevno skeniranje računala, korištenje antivirusnih softvera, biometrijske identifikacije, sustava za otkrivanje upada i višenamjenskih sustava provjere autentičnosti. Što se tiče korištenja zaporki, 69% ispitanika je upoznato s korištenjem jednostavnih zaporki ili ih svjesno koristi. Na pitanje koliko često koriste jednostavne lozinke, 64% studenata navodi kako ih koristi više od pedeset posto vremena, što u ovom slučaju i nije tako impresivno s obzirom da je čak i jednostavna lozinka neophodna kako bi neki podatci bili sigurni i održali integritet sustava. Što se tiče sofisticiranih zaporki, čak 87% ispitanika nije upoznato s takvim načinom zaštite i načinom na koji se formiraju pa je pretpostavka da ih zato i manje koriste, a na pitanje koliko često koriste sofisticirane zaporke oni koji koriste, njih 90% ih koristi manje od 3% vremena. U ovom slučaju, nepoznavanje korištenja sofisticiranih zaporki može se tumačiti kao ne-uporabu, što je razumljivo jer poznavanje mora prethoditi upotrebi. Autori Lomo-David i suradnici (2009) u skladu s dobivenim rezultatima preporučuju obrazovnim institucijama kako bi trebale još više informirati studente o korištenju sigurnosnih mjera na računalima. Mensch i Wilkie (2011) uspoređivali su sigurnosne prakse studenata s obzirom na spol, dob, socioekonomski status, a ispitani su stavovi studenata vezano za upravljanje zaporkama za *online* račune, instalaciji i

uporabi antivirusnog softvera, instalaciji i uporabi antispam softvera, otvaranju veza unutar e-pošte ili izravnih poruka, korištenja bežičnog računalstva, krađa identiteta itd. Studentima preddiplomskog i diplomskog studija ponuđena je mogućnost sudjelovanja u istraživanju, a od njih 2000, u istraživanju je pristalo sudjelovati 127 studenata. Ispitanici su putem e-pošte dobili poveznicu i popunjavali online anketu. Najviše sigurnosnih ponašanja u odnosu na dob pokazuju najmlađi sudionici, od 18 do 23godine (M = 85,97), dok najmanje sigurnosnog ponašanja iskazuju stariji studenti od 24 do 30 godina (M = 79,94). Većina sudionika nije bila žrtva krađe identiteta (85,8%), imaju instaliran antivirusni softver (80,3%), kao i instaliran *antispywarwe* na svojim računalima (74,8%). Međutim, 70,9% sudionika gotovo nikada ili nikada ne pokreće antivirusni softver na USB memorijskim uređajima, a samo 11% to čini uvijek ili većinu vremena. Kada je riječ o informacijskoj sigurnosti, Mensch i Wilkie (2011) smatraju kako bez obzira na postojanje sve sofisticiranijih tehnoloških rješenja, krajnji korisnik mora naučiti prihvatiti odgovornost i poduzeti proaktivne mjere kako bi ostao educiran o dostupnim sigurnosnim alatima i procedurama za zaštitu osobnih podataka i informacija na mrežnim i izvanmrežnim mjestima.

Siponen (2000) smatra kako sadašnji pristupi u pogledu informacijske sigurnosti i obrazovanja nisu orijentirani na dostignuće niti prepoznavanje činjenica, a trenutne studije ne istražuju mogućnosti koje nude teorije motivacije i ponašanja. Prva pretpostavka, razina deskriptivnosti, smatra se upitnom, jer na kraju može dokazati da krajnji korisnici ne uspijevaju internalizirati zadane ciljeve i, primjerice, ne slijede sigurnosne smjernice - što je neprimjereno. Autor Siponen (2000) smatra kako se uloga motivacije u području informacijske sigurnosti ne smatra dovoljno ozbiljnom, iako je njezina uloga široko priznata.

U istraživanju koje su provodili Er i sur. (2017) sudjelovali su studenti privatnog sveučilišta u dobi od 19 do 24 godine. Cilj je bio odrediti razinu svijesti o pitanjima *cyber* sigurnosti i njihovoj sposobnosti da se zaštite od rizika na internetu. Korištene su i kvalitativne i kvantitativne metode istraživanja. Anketni upitnik korišten je kako bi se utvrdila njihova svijest i razumijevanje problema *cyber-sigurnosti* i sposobnost zaštite od rizika. Intervju fokusnih skupina korišten je za ispitivanje percepcije i iskustva studenata o rizičnim *online* aktivnostima. Rezultati pokazuju sljedeće: (i) studenti su se osjećali prilično sigurno kada su bili na internetu (ii) imaju dobro razumijevanje onoga što predstavlja rizične online aktivnosti (iii) studenti također znaju kako se zaštititi tijekom korištenja interneta (iv) unatoč tome, još uvijek prepoznaju važnost učenja o sigurnosti na internetu. Ovo istraživanje dio je kontinuiranog niza istraživanja na različitim područjima koja imaju za cilj identificirati razinu svijesti o sigurnoj i odgovornoj uporabi ICT-a .

Istraživanje Robertsona i suradnika (2001) uključivalo je studente druge godine studija (16 studenata), te srednjoškolce (15 maturanata). Dob za srednjoškolsku grupu kretala se od 17 do 18 godina, a za sveučilišnu skupinu od 18 do 42 godine, uključujući osam studenata preko 30 godina. Ukupni uzorak (N=31) uključivao je šesnaest muškaraca i petnaest žena. Svi su studenti imali račune e-pošte, a većina je imala kućna računala, iako ne uvijek i vezu s internetom. Kada su im postavljena pitanja vezana uz osobnu sigurnost, ponovno su istaknute neke jasne razlike između sudionika maturanata i studenata. Kada se pitaju o osobnoj sigurnosti, studenti vide svojevrsne opasnosti i znaju da potpuna anonimnost u konačnici nije moguća. Nasuprot tome, čini se da maturantima nedostaje takvo razmišljanje.

Hall (2012) je pokušao utvrditi kakva je percepcija studenata o važnosti očuvanja osobnih podataka i njezina digitalna dostupnost. U istraživanju su sudjelovali studenti informatike koji su već imali neke od predmeta kao što su društvene mreže, mediji, nove tehnologije i sl. dok je druga grupa studenata bila „ne tehničarska", odnosno uključivala je studente kriminologije koji nisu imali toliko predmeta koji su pokrivali ovo područje informatike. Rezultati do kojih je Hall (2012) došao navode kako se 57% studenata ne brine ili se malo brine zbog osobnih podataka dostupnih na internetu, dok je 50% spremno ostaviti računala „prijavljena" dulje vrijeme. Međutim, 90% koristi neki oblik privatnosti, a 56% ne koristi javna računala iz osobnih razloga. „Ne tehničarska" skupina studenata bila je još manje zabrinuta zbog dostupnosti informacija, ali je više pazila kada bi napuštala računalo. Iako su studenti uglavnom nezabrinuti jer su njihovi osobni podatci digitalno dostupni, vode brigu da ih ipak mogu kontrolirati na neki način. Podatci upućuju da su studenti samo blago svjesni kako postoji potencijalna opasnost od zlouporabe ili neetičnih akcija temeljenih na njihovim digitalnim informacijama. Pretpostavka je da bi ti brojevi bili vrlo različiti kada bi se više njih osobno ili profesionalno „opeklo" zbog zlouporabe svojih digitalnih informacija ili ako bi točno znali koje su informacije dostupne. Osobito ako 50% njih napušta račune aktivnima (ne odjavi se), a koristi javna računala za osobne potrebe.

Istraživanja među studentima u Republici Hrvatskoj rađena su također s ciljem utvrđivanja njihovih stavova i mišljenja o sigurnosti na internetu, mogućim opasnostima, zlouporabi, te zaštiti identiteta. Vrana (2013) je u svom radu prikazao rezultate istraživanja studenata Filozofskog fakulteta u Zagrebu, njihova stajališta i mišljenja o sigurnoj uporabi društvenih mreža. Istraživanje je provedeno u ožujku 2013. godine s ukupno 197 studenata koji su dobrovoljno sudjelovali u istraživanju. Iako se može reći da je ovaj broj studenata možda nedovoljan, još uvijek ukazuje na neke važne trendove korištenja interneta u cjelini i na mrežnim društvenim mrežama. Rezultati pokazuju da je većina ispitanika iskusnih

korisnika društvenih mreža, međutim, rijetko mijenjaju zaporke u mrežnim profilima, a većina njih nikada nije imala nikakvo obrazovanje općenito o sigurnosti na internetu i načinu zaštite osobnih podataka na društvenim mrežama. Srećom, većina njih nikada se nije susrela s provalama na svoje profile na društvenim mrežama. Općenito govoreći, studenti su vrlo zainteresirani za korištenje mrežnih društvenih mreža i čini se da ih ništa neće spriječiti da tako nastave u budućnosti. Međutim, trebali bi uložiti više vremena u obrazovanje o sigurnoj upotrebi društvenih mreža i primijeniti zdrav razum pri prihvaćanju sadržaja drugih ljudi koji su im poznati i onih koji se pretvaraju da su njihovi prijatelji kako bi se zaštitili. Buduća istraživanja mogu uključivati druge skupine čestih korisnika mrežnih društvenih mreža kako bi istražili postoji li isti obrazac korištenja mrežnih društvenih mreža kao kod studenta na Filozofskom fakultetu u Zagrebu.

Autori Velki, Šolić i Očevćić (2014) su željeli razviti opći upitnik za ispitivanje informacijske sigurnosti korisnika (UZPK). Razvoj upitnika se sastojao od odabira prikladnih čestica za koje se pretpostavlja da mjere razinu znanja o informacijskoj sigurnosti te rizična ponašanja računalnih korisnika. Upitnik se sastojao od dva dijela s ukupno 37 čestica. Sudionici ove studije bili su studenti (N = 135) na drugoj godini preddiplomskog studija, s tri različita fakulteta Sveučilišta J. J Strossmayera u Osijeku. Dobiveni rezultati su optimistični, jer upitnik UZPK-a ima potencijal postati priznat i pouzdan upitnik za mjerenje svjesnosti o sigurnosti informacijskih korisnika. U svakom slučaju IT stručnjaci moći će analizirati korisnike informacijskih sustava kako bi se identificirali problemi s niskom razinom sigurnosti, a znanstvenici će moći općenito kategorizirati korisnike informacijskih sustava u pogledu razine svijesti o njihovoj informacijskoj sigurnosti. Analizom dovoljno uzoraka svih vrsta korisnika informacijskih sustava trebalo bi biti moguće dobiti neke opće zaključke o potencijalno rizičnom ponašanju korisnika, korelaciji s razinom sigurnosti i identifikacijom većine nesigurnih vrsta korisnika. Kranji cilj autora je razvoj validirane međunarodne verzije UZPK-a, koja je između ostaloga, omogućila i primjenu upitnika za mjerenje svjesnosti o sigurnosti zaposlenika prilikom korištenja IKT-a na poslu, o čemu će biti riječi u slijedećem poglavlju.

2.1.1.2. Pregled istraživanja o sigurnosti zaposlenika na internetu

Pitanja s kojima se susreće veliki broj poduzeća u svijetu je pitanje zaštite povjerljivosti, integriteta i dostupnosti informacija. Upotrebom novih tehnologija postoje novi informacijski rizici koji mogu dovesti do „curenja“ podataka, poteškoća u kontinuitetu poslovanja, reputacijski rizici kroz gubitak vrijedne intelektualne imovine, povjerenje potrošača i konkurentske prednosti.

Hagen i Albrechtsen (2009) u svom su radu nastojali mjeriti i raspraviti učinke alata za e-učenje s ciljem poboljšanja znanja, svijesti i ponašanja zaposlenika o informacijskoj sigurnosti. Pomoću eksperimenta, procjenjivali su se stavovi zaposlenika prije i nakon intervencije. Ukupno 1897 djelatnika odgovorilo je na anketu prije i nakon intervencije. Uzorak je podijeljen na intervencijsku i kontrolnu skupinu, pri čemu je jedina razlika između ovih dviju skupina bila sudjelovanje u intervenciji (tj. korištenje alata za e-učenje). Rezultati istraživanja ukazuju na značajna kratkotrajna poboljšanja u znanju i ponašanju članova eksperimentalne skupine. Studija je utvrdila kako softver koji podržava programe informiranja o sigurnosti informacija ima kratkotrajni učinak na znanje, ponašanje i svijest zaposlenika. Rad je inovativan u području istraživanja informacijske sigurnosti jer pokazuje kako se mogu mjeriti učinci intervencije na informacijsku sigurnost.

Pojam koji se vrlo često povezuje u istraživanjima vezano uz sigurnost zaposlenika na internetu je socijalni inženjering koji podrazumijeva manipuliranje ljudima u svrhu otkrivanja povjerljivih informacija ili pristupa resursima do kojih manipulator ne može sam doći. Autori Wilcox, Bhattacharya i Islam (2014) proučavajući utjecaj socijalnog inženjeringa na ugled kompanija, naglašavaju kako socijalni inženjering napada najslabiju organizacijsku sigurnosnu vezu - čovjeka. Sve veći je broj zaposlenika koji koriste društvene medije u radnom okruženju što stavlja stručnjake za informacijsku sigurnost pred velike izazove. Brojne su studije (Gross i Acquisti, 2005; Meister i Willyerd, 2010; Furnell, 2008; prema Wilcox i sur., 2014) pokazale kako postoji rastuća povezanost socijalnog inženjeringa i društvenih medijskih stranica kao što su Facebook i Twitter, zbog bogatstva osobnih i organizacijskih informacija koja se nalaze u tim okruženjima. Ti izazovi također pokazuju izuzetno velik utjecaj na povjerljivost, integritet i dostupnost informacijske imovine koja se nalazi unutar organizacije. Wilcox i sur. (2014) su u istraživanju željeli prikazati dubinski uvid u klasifikaciju i načine smanjivanja socijalno inženjerskih sigurnosnih pitanja s kojima se suočavaju kompanije kod korištenja društvenih medija za poslovnu uporabu. Autori smatraju kako su zaposlenici ključni za reputaciju organizacije, ali ako objavljuju neprikladne ili netočne komentare, osobito ako su u suprotnosti s korporativnom porukom kompanije, oni također mogu uzrokovati štetu s ogromnim posljedicama po ugledu kompanije. Drugo gledište koje se odnosi na gubitak ugleda koji bi se mogao pojaviti izvan službenih ili profesionalnih računa jest šteta koju uzrokuje forumska aktivnost u kojoj potrošači govore o sviđanju ili ne sviđanju određenoga poduzeća. Wilcox i sur. (2014) smatraju kako je najučinkovitija sigurnosna mjera protiv socijalnog inženjeringa povećati svijest zaposlenika o mnogim trikovima koje socijalni inženjeri koriste protiv njih na radnome mjestu.

U pregledu istraživanja vezano za ponašanje zaposlenika po pitanju sigurnosti informacijskih sustava u zadnjem desetljeću, Lebek i sur. (2014) su analizirali 113 publikacija i smatraju kako bi se buduće empirijske studije trebale usredotočiti na dodatne čimbenike koji utječu na svijest o informacijskoj sigurnosti zaposlenika i njihovo ponašanje. Iako je prisutna dominantnost kvantitativnih istraživanja, Lebek i sur. (2014) mišljenja su kako nedostaju kvalitativna istraživanja u vidu akcijskih istraživanja i intervjua, što može dodati vrijednost ovome istraživačkom polju sigurnosti.

Istraživanja koja se bave sigurnošću zaposlenika na internetu, nisu vrlo česta u Republici Hrvatskoj, međutim Velki, Šolić i Nenadić (2015) razvili su valjan i pouzdan instrument koji mjeri utjecaj korisnika na sigurnost informacijskoga sustava, Upitnik znanja i rizičnog ponašanja korisnika informacijskog sustava (UZPK; Velki i Šolić, 2014; prema Velki, Šolić i Očević, 2014). Istraživanje je provedeno u tri navrata prikupljanja podataka. Prvi se uzorak sastojao od 135 studenata druge godine preddiplomskoga studija na kojemu je provjerena konstruktna valjanost, pouzdanost i osjetljivost pojedinih subskala te odabrane odgovarajuće čestice. Drugi se uzorak sastojao od 211 studenata i zaposlenika, a na njemu su provjerene metrijske karakteristike poboljšanog instrumenta te je dobivena konačna verzija. Treći se uzorak sastajao od 152 zaposlenika i na njemu je validiran UZPK. Autori Velki, Šolić i Nenadić (2015) došli su do zaključka kako studenti, u odnosu na zaposlenike, statistički značajno češće brinu o održavanju računalnih sustava, što je i očekivano jer se radi o studentima Elektrotehničkoga fakulteta, kojima je to sastavni dio obrazovanja. Sukladno očekivanom, zaposlenici procjenjuju komunikaciju računalom manje sigurnom za razliku od studenata koji komunikaciju putem računala vjerojatno koriste u različite svrhe (npr. upoznavanje, druženje, razmjena informacija i sl.) i ne uzimaju u obzir sve potencijalne opasnosti, već su usmjereni na prednosti elektroničke komunikacije. Također je moguće da posjeduju i dodatna znanja kako zaštiti svoj računalni sustav, pa stoga ovu vrstu komunikacije smatraju sigurnijom. Na trećem je uzorku zaposlenika dobivena i jedna statistički značajna razlika između muškaraca i žena. Muškarci, za razliku od žena, smatraju da je komunikacija računalom sigurnija. Moguće da je dobivena razlika odraz društva u kojemu živimo, ali i stvarnih situacija u kojima su žene češće žrtve zlouporabe i internetskoga nasilja (West, 2014, prema Velki i sur., 2015), pa ne iznenađuje da one procjenjuju internetsku komunikaciju manje sigurnom. Dobivena je dobra konstruktna valjanost Upitnika, sve skale i subskale imaju zadovoljavajuće metrijske karakteristike (pouzdanost i osjetljivost) te je dobivena i dobra kriterijska valjanost tako da se može reći kako Upitnik predstavlja valjan i pouzdan mjerni instrument, zadovoljavajućih psihometrijskih karakteristika.

Nadalje u Republici Hrvatskoj, u povodu „Europskog mjeseca kibernetičke sigurnosti 2017" predstavljeno je redovno godišnje istraživanje Hrvatske udruge banaka o stanju sigurnosti na internetu. Anketa provedena na uzorku od tisuću ljudi iz cijele Republike Hrvatske, a s namjerom da se utvrdi stupanj osjećaja ugroženosti i razinu osviještenosti kod građana o potrebi sigurnosne zaštite tijekom obavljanja uobičajenih aktivnosti na internetu, s posebnom naglaskom na preuzimanje internetskoga sadržaja putem mobitela. Riječ je o aktivnostima kao što su uporaba e-pošte, komunikacija putem društvenih medija, pristup internetu putem besplatnih, nezaštićenih bežičnih (Wi-Fi) mreža, samozaštita pri obavljanju transakcija putem mobilnog bankarstva, paze li koje stranice na internetu posjećuju i preuzimaju li aplikacije za mobitel samo s regularnih trgovina (App Store, Google Play) ili riskiraju nepotrebno negdje drugdje.

2.2. PRIVATNOST I OSOBNI PODATCI NA INTERNETU

Kao odrasle osobe, mi smo ti koji određujemo koliko će dijete imati pristup digitalnim alatima i kako su njegovi osobni podatci zaštićeni. Zaštita osobnih podataka u Republici Hrvatskoj te nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka u Republici Hrvatskoj uređuje se Zakonom o zaštiti osobnih podataka („Narodne novine", broj 103/03, 118/06, 41/08, 130/11, 106/12-pročišćeni tekst). Svrha zaštite osobnih podataka je zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka. Zaštita osobnih podataka u Republici Hrvatskoj osigurana je svakoj fizičkoj osobi bez obzira na državljanstvo i prebivalište te neovisno o rasi, boji kože, spolu, jeziku, vjeri, političkom ili drugom uvjerenju, nacionalnom ili socijalnom podrijetlu, imovini, rođenju, naobrazbi, društvenom položaju ili drugim osobinama.

Zakonom o zaštiti osobnih podataka osnovana je Agencija za zaštitu osobnih podataka kao samostalno i neovisno tijelo s temeljnom zadaćom provedbe nadzora nad obradom osobnih podataka u Republici Hrvatskoj.

2.2.1. KAKO POVEĆATI SIGURNOST PRI KORIŠTENJU MOBILNIH UREĐAJA?

Posljednjih godina neki oblici IKT-a, poput mobilnih telefona, su postali pristupačni svima i danas omogućuju lak pristup informacijama, ljudima, uslugama i dobrima. Townsend (2010) navodi kako je širenje mobilne telefonije među najbržim inovacijama ikad. Slično kao računala, tableti i mobiteli lako se mogu zamijeniti i trebaju biti osigurani kako bi jamčili sigurnost pojedincu i ustanovi.

Prema podatcima Međunarodne telekomunikacijske unije (2017) do kraja 2017. godine bilo je gotovo 7 milijardi mobilnih telefonskih pretplata na globalnoj razini, s oko 4,5 milijardi jedinstvenih pretplatnika i oko 3 milijarde ljudi (40 posto svjetske populacije) imalo je pristup internetu putem mobilnih i / ili fiksnih širokopojasnih pretplata (International Telecommunication Union, 2017).

Beth i sur. (2014) proveli su istraživanje na jednom sveučilištu SAD-u u kojem je sudjelovalo 500 studenata ekonomije. U radu se opisuje istraživanje o stupnju sigurnosti koju studenti prakticiraju prilikom korištenja pametnih telefona. Cilj ovoga istraživanja bio je dobiti uvid u ključna motrišta studentskog ponašanja pri korištenju mobilnih tehnologija. Dok se studenti često oslanjaju na više vrsta mobilnih uređaja, opseg istraživanja bio je ograničen na korištenje pametnih telefona. Rezultati ove ankete pokazuju veliku razliku u praksi među studentima. Dok se neki studenti bave nekim motrištima sigurnosti pametnih telefona, oni i dalje ostaju ranjivi na napad: 44% nije bilo suglasno da je korištenje zaporke važno, manje od trećine odjavljuje se s e-pošte i društvenih mreža kada ih ne koriste, oko polovice nije izgledalo neodlučno otvoriti privitak iz nepoznatog izvora, samo 40% ograničilo je svoje Wi-Fi aktivnosti na zaštićene mreže.

Slično kao u svijetu i u Republici Hrvatskoj je velik porast preuzimanja internetskoga sadržaja putem mobitela. Mobitel postaje sve traženija platforma pa tako i u bankarstvu - u Hrvatskoj bilježimo oko 600.000 tisuća korisnika mobilnog bankarstva, istaknuo je predstavljajući istraživanje direktor Hrvatske udruge banaka Zdenko Adrović i naglasio: „U digitalnom dobu, u koje postupno i neupitno ulazimo, sigurna zaštita podataka i komunikacije postaju sve važnije za građane i tvrtke, a posebno za financijski sektor čije se poslovanje svodi na povjerenje koje klijenti imaju u banke. Zato će zaštita i edukacija o kibernetičkoj sigurnosti za nas ostati prioritet."

Na koji način povećati sigurnost pri korištenju mobilnih telefona navodimo preporuku koju su dali Internet Crime Complaint Center (IC3), u suradnji s Federalnim zavodom za istrage (FBI) i National White Collar Crime Center (NW-CCC), (IC3, 2012) prema Beth i sur. (2014):

- Isključiti značajke koje nisu potrebne. Koristiti šifriranje (ako je dostupno) za zaštitu osobnih podataka.
- Pogledati recenzije razvojnog programera / tvrtke koja je objavila aplikaciju.
- Pregledati i razumjeti dozvole koje dajemo prilikom preuzimanja aplikacija.
- Koristiti zaštitu lozinkom.
- Dobiti zaštitu od zlonamjernog softvera.
- Imati na umu aplikacije koje omogućuju Geo-lokaciju.

- Ne zatvarati jailbreak (jailbreak ili rooting koristi se za uklanjanje određenih ograničenja proizvođača uređaja ili mobilnog telefona.)
- Ne povezivati se s nepoznatim bežičnim mrežama.
- Obrisati sve na uređaju (resetirati ga na tvorničke postavke) prilikom prodaje ili mijenjanja.
- Koristiti ažuriranja.
- Izbjegavati otvaranje softvera ili poveznica iz nepoznatih izvora.
- Upotrijebiti iste mjere opreza na mobilnom telefonu kao i na računalu prilikom korištenja Interneta.

U Republici Hrvatskoj prema *Izvješću Hrvatske udruge banaka o stanju sigurnosti na Internetu za 2016. godinu* (2017), u slučajevima kada se susretnu s porukom (e-pošta, SMS) nepoznatog pošiljatelja, koja ih navodi na primamljivu ponudu i nosi u sebi poveznicu prema nekom mrežnom odredištu – 93% ljudi će takvu poruku ignorirati i odmah obrisati, a preostalih 7% će riskirati i na neki način nastaviti baviti se tom porukom. Što se tiče besplatnog, nezaštićenog, bežičnog pristupa internetu (Wi-Fi) čak 37% ljudi ih koristi kad god može, 31% ih se Wi-Fi mrežama koristi povremeno, a 32% uopće ne koristi besplatni bežični pristup internetu. Oni koji koriste Wi-Fi, koriste ga uglavnom kao metodu štednje - smanjenja troška prijenosa podataka na mobilnoj mreži koju koriste. Na tim mrežama rade ono što i inače rade kad su na internetu: čitaju vijesti, komuniciraju e-poštom i druže se na društvenim mrežama. Dobra vijest je da među onima koji Wi-Fi koriste bilo često ili samo povremeno, ima samo tri posto onih koji putem tih nezaštićenih otvorenih veza pristupaju mobilnom bankarstvu.

Sudionici istraživanja, iako među njima ima još uvijek previše neopreznih, pokazali su dosta opreza pri pregledavanju internetskoga sadržaja koji ih zanimaju na mreži nad mrežama. Njih 55% ne otvara internetske stranice za koje nisu sigurni da su autentične. Međutim, čak 34% sudionika ankete, o pouzdanosti mrežnih odredišta koje posjećuju uopće nije razmišljalo. Većini je najvažnije da su sadržaji koji ih zanimaju lako i jednostavno dostupni putem mobitela. Što se tiče preuzimanja aplikacija, 56% ispitanika preuzima aplikacije samo putem trgovina koje ponudi mobitel, no njih 34% uopće ne preuzima nikakve aplikacije na mobitele.

2.2.2. SIGURNOST I ZAŠTITA KORISNIČKOG IMENA I ZAPORKE

Ovisno o društvenoj mreži, e-pošti kojom se koristite ili bilo kojom stranicom koja zahtijeva upotrebu korisničkog imena i zaporke, važno je da one budu

dobro odabrane kako biste spriječili da se netko drugi koristi vašim korisničkim profilom. Odabir kvalitetne sigurnosne zaporke ponekad nije jednostavan, stoga donosimo savjete kako odabrati najbolju.

Kad je u pitanju uporaba zaporki pri komunikaciji putem e-pošte ili društvenih mreža, u Republici Hrvatskoj prema *Izvješću Hrvatske udruge banaka o stanju sigurnosti na internetu za 2016. godinu* (2017), 59% ispitanika zaporke mijenja jednom godišnje ili rjeđe, a 34% samo kada zaborave staru zaporku. Uz to, znatno je pao broj ljudi koji redovito mijenjaju zaporku – sa 16% u svibnju 2016., na samo sedam posto u rujnu 2016.

Laka pamtljivost zaporka - pobrinite se da je zaporka nešto što možete zapamtiti. Najbolje je odabrati nešto specifično kako biste to uvijek imali na umu, ali opet ne toliko preočito da je može svatko pogoditi. Odaberite neki vama pamtljiv dugačak izraz ili izreku te zaporku kreirajte od cijeloga izraza ili samo od njegovih prvih slova. Primjerice, preuzimanjem početnih slova svake riječi poslovice „Tko rano rani dvije sreće grabi" dobijete „trrdsg" te tome dodajte poneko veliko slovo i broj te vaša zaporka može biti "tRr7DsG".

U istraživanju Sharples i sur.(2009) zamolili su ispitanika da predlože zaporku od najmanje šest znakova koje nisu prije upotrebljavali, ali za koje misle da se mogu sjetiti za pristup tom istraživanju. Izbor zaporke ukazuje na koji način ispitanici pristupaju sigurnosti na internetu. Polovica ispitanika dala je zaporku temeljenu na osobnim podatcima kao što su datum rođenja ili ime člana obitelji koji se može naći iz osobnih evidencija. Daljnjih 25% koristilo je zaporku koja se može naći u rječniku. To ukazuje na zabrinjavajući nedostatak sigurnosti (iako nema dokaza da su njihovi rezultati lošiji od odrasle populacije) ipak postoji jasna potreba da se pomogne djeci razumjeti rizike nesigurnih zaporki i kako ih spriječiti.

Jednostavnost zaporke - izbjegavajte jednostavne zaporke poput 123456, abcdefg i slično ili bilo koju riječ sadržanu u nekom od „rječnika zaporki". Naime, postoje liste riječi za koje hakeri znaju da se često koriste kao lozinke poput raznih pojmova iz astrologije, biologije, crtanih filmova, sporta, filmova, mjesta, znanstvene fantastike i slično.

Korištenje iste zaporke - ne koristiti istu zaporku za sve postojeće račune. Poznat je primjer lažnih servisa za dijeljenje podataka koji su postavljeni samo u svrhu upada u račune korisnika. Slični servisi traže registraciju korisnika u nadi da će upisati istu zaporku, a koja će se onda moći iskoristiti za pristup njihovim podatcima.

Zapisivanje zaporke – zaporke su inače vrlo kratke te njihova duljina obično iznosi minimalno šest znakova. Ukoliko niste sigurni da ćete ih ipak sve zapam-

titi, zapišite ih negdje gdje nitko drugi nema pristup. Zapis u računalu ipak nije najbolji odabir, posebice zbog mogućnosti njegova tehničkoga kvara. Najbolje je zapisati lozinku u neku bilježnicu koju držite na mjestu zajedno s vašim važnijim dokumentima.

Kad je u pitanju čuvanje zaporke kojima se pristupa uslugama mobilnog bankarstva, prema Izvješću Hrvatskih banaka, 52% sudionika ankete tvrdi da te podatke znaju samo oni i da ih nemaju nigdje pohranjene, a 29% ih o tome ne razmišlja. U odgovoru na ovo pitanje pokazale su se statistički značajne razlike prema dobi. Mlađi ljudi bolje čuvaju zaporke za mobilno bankarstvo od starijih. Štoviše, stariji te zaporke zapisuju na više mjesta (Hrvatske udruga banaka, 2017).

Kombinacije na tipkovnici - ne koristiti kombinacije na tipkovnici poput asqw12, yxasqw, i slično ili neke uobičajene zaporke uz tipku „shift", poput primjerice zaporku „!"#$%&/" koja možda djeluje sigurno, ali je zapravo riječ o znakovlju "shift + 1234567", što većina rječnika koji se koriste za provaljivanje lozinki sadržava u sebi.

Kombinacija veličine slova - kod sistema koji prepoznaju razliku između velikih i malih slova, koristite obje veličine slova u kreiranju zaporke. Čak i ako se odabere jednostavan pojam za zaporku, raznovrsnost veličine znakova znatno će otežati pristup nekome tko želi ući u vaše korisničke račune.

Vlastiti algoritam - koristite vlastiti „algoritam" za kreiranje zaporke. Primjerice, odabrati prva četiri znaka iz imena stranice na koju se registrirate i dodati zadnje četiri znamenke broja telefona nekog prijatelja. Navedeni algoritam može se dodatno razraditi tako da se od svakog slova odabere sljedeće ili prethodno slovo u abecedi, kombiniranjem velikih i malih slova i slično. Također može se ubacite neko veliko slovo, i to najbolje negdje u sredini riječi, a ne na početku (npr. stoLica). Zatim umjesto slova o ubaciti broj 0, a umjesto slova a staviti @ (st0Lic@). Može se dodati na kraju znak ! (st0Lic@!). Moguće je i neku riječ zapisati unazad, npr. stolica = acilots. Iako nema smisla, ali je dovoljno da zapamtite pojam za koji ste se opredijelili. Što je više koraka u kreiranju algoritma, to je zaporka sigurnija. Prednost ovakvog načina stvaranja zaporki, osim njihove sigurnosti i različitosti, jest i pamtljivost jer je dovoljno zapamtiti način na koji kreirate zaporke da biste znali veliki broj istih napamet.

Poticanje informatičke pismenosti, računalne i komunikacijske tehnologije postalo je dio svakodnevnog života. Zbog raznih opasnosti koje nude elektronički mediji, važno je pravovremeno prepoznati i spriječiti neželjene događaje. Važno je educirati djecu i mlade o preuzimanju odgovornosti za svoje ponašanje i o posljedicama određenih postupaka putem interneta, kao i o sigurnosnim pravilima kako bi se zaštitila njihova prava, interesi i aktivnosti.

2.3. ZA RAZMIŠLJANJE ...

- Thierer (2009) navodi primjer kako je u SAD-u imenovano pet radnih skupina sastavljanih od stotine stručnjaka iz cijeloga svijeta koji se bave sigurnošću djece na internetu, svih pet skupina složilo se oko zajedničkih zaključaka/preporuka koje su se nametnule u svim skupinama:
- Obrazovanje je primarno rješenje za većinu internetskih problema vezanih uz sigurnost djece, naglašavajući važnost medijske pismenosti i napora u osvješćivanju javnosti, javnih službi, primjena ciljanih intervencijskih tehnika i bolja strategija mentorstva i roditeljstva.
- Ne postoji „čarobni štapić" kojim bi se riješila zabrinutost vezana za sigurnost djece, naročito u vremenu brzih promjena u digitalnom svijetu.
- Osnaživanje roditelja i skrbnika pomoću različitih alata može pomoći obiteljima i školama više kontrolirati *online* sadržaje i komunikaciju.
- Tehnološki alati i roditeljski nadzor najučinkovitiji su dio složenog pristupa sigurnosti djece, koji ih smatra jednim od mnogih strategija ili rješenja.
- Najbolje tehničke mjere kontrole su one koje zajedno s obrazovnim strategijama i pristupima vode dijete i mentoriraju ga. Stoga, tehnička rješenja mogu nadopuniti, ali nikada zamijeniti, ulogu obrazovanja i mentoriranja.
- Kreatori politika trebali bi se usredotočiti na poticanje kolaborativnih, višestranih inicijativa i pristupa kako bi se poboljšala sigurnost na internetu. Dodatni resursi za obrazovanje i napore za izgradnju svijesti također su presudni.
- Na kraju, države bi trebale osigurati odgovarajuće kazne za kažnjavanje teških kaznenih djela protiv djece i osigurati da agencije za provedbu zakona imaju odgovarajuća sredstva za privođenje i kažnjavanje zločinaca. (Thierer, 2009)

2.4. KORISNE POVEZNICE

U Republici Hrvatskoj postoje danas već brojni projekti, udruge i organizacije koje se bave sigurnošću na internetu, ovdje donosimo pregled nekih od njih kako bi vam olakšali snalaženje u pronalasku edukativnih brošura, prezentacija, radionica, aplikacija, obrazaca za uklanjanje osobnih podataka s društvenih mreža…

→ Na mrežnoj stranici Agencije za zaštitu osobnih podataka možete pronaći obrasce za uklanjanje osobnih podataka s društvenih mreža (prijava lažnog pro-

fila na Facebooku, prijava lažnog profila na Instagramu, uklanjanje videozapisa sa You Tubea, zahtjev prema Googleu za uklanjanje rezultata pretraživanja o fizičkoj osobi)

http://azop.hr/zahtjevi-za-uklanjanje-osobnih-podataka/ (Pristupljeno 6.11.2018.)

→ Agencija za zaštitu osobnih podataka izradila je niz promotivnih i edukativnih materijala vezanih za zaštitu osobnih podataka namijenjenu djeci, roditeljima i ostalim građanima.

- *Vodič ICC-a za informacijsku sigurnost u poslov*anju
- Letak *Korištenje kanala dpacasework@fb.com-obraćanje Facebooku*
- Letak *Deset najčešćih upita o zaštiti privatnosti na Facebooku*
- Brošura *Safety@Facebook*
- Letak *Prava potrošača u sustavu zaštite osobnih podataka u RH*
- Brošura *Zaštita podataka - Bolja pravila za mala poduzeć*a
- Letak *Opća Uredba o zaštiti osobnih podataka*
- Brošura *Privatnost djece i mladih u svijetu modernih tehnolo*gija
- Letak P*rivatnost - zašita osobnih podataka građana*
- Vodič za voditelje zbirki osobnih podataka
- Vodič za građane EU - SAD *Štit privatnosti*
- Brošura *Zaštita osobnih podatka u RH*
- Brošura *Zaštita privatnosti na radnom mjestu*
- Brošura *Sigurno surfanje: zaštita osobnih podataka na internetu*
- Brošura *Moja Fejs priča*
- Letak *Ne budi meta kradljivaca identiteta*
- Letak *Zaštita osobnih podataka djece na internetu*
- Letak *Zaštita osobnih podataka djece na društvenim mrežama*
- Letak *10 koraka protiv govora mržnje na internetu*
- Letak *Bolja zaštita vaših osobnih podataka*

http://azop.hr/info-servis/detaljnije/promotivni-materijali/ (Pristupljeno 6.11.2018.)

→ CARNET- hrvatska akademska i istraživačka mreža, na svojim stranicama posebno posvećuje pozornost sigurnosti na internetu gdje možete pronaći brošure namijenjene mladima, osnovne korake zaštite računalne infrastrukture poduzeća od sigurnosnih rizika. Savjeti su posebno prilagođeni prioritetima i zadaćama računala u poslovnom okruženju. Neke od obrađenih tema su zaštita tajnosti podataka, izrada sigurnosne politike te sigurnosno podešavanje poslužitelja javnih usluga. Opasnostima kojima se izlažete prilikom postavljanja osobnih podataka i sadržaja na najpopularniju društvenu mrežu te kako podesiti svoj profil na Fejsbooku tako da čuva privatnost.

- Brošura *Zaštitite privatnost na Facebooku*
- Brošura *Sigurnije na internetu*
- Brošura *Sigurnije poslovanje na internetu*

http://www.carnet.hr/sigurnost (Pristupljeno 6.11.2018.)

→ Antibot.hr je besplatan servis kojeg pruža CARNet zajedno s tvrtkama partnerima. Namjena antibot.hr servisa je smanjenje broja zaraženih računala, tableta i pametnih telefona kao i pomoć korisnicima pri čišćenju vlastitih uređaja za pristup internetu od zlonamjernih programa. Ovdje možete pronaći pregled općenitih informacija i savjeta o prijetnjama na internetu te prijedlozima za zaštitu (*phishing, ransomware*, neželjene poruke, sigurne zaporke, internet bankarstvo, siguran WLAN).

http://www.antibot.hr/ (Pristupljeno 6.11.2018.)

→ Centar za nestalu i zlostavljanu djecu neprofitna je udruga osnovana 2006. god. u Osijeku. Motiv za osnivanjem Centra osnivači su prepoznali u problemima nedovoljne zaštite djece od seksualnog iskorištavanja i zlostavljanja putem interneta te širenja dječje pornografije i pedofilije, ali i drugih oblika zlostavljanja vezanih uz uporabu interneta.

Edukacijski paket za Dan sigurnijeg interneta 6.2.2018. sadrži:

Djeca i mladi

- Društvena igra (PDF)
- Edukacijski paket - radionice (PDF)

Nastavnici i roditelji

- *Cyberbullying* (PPT)
- Priručnik prevencija nasilja putem interneta
- Program edukacije - *Mediji današnjice*

Promotivni materijali

- 10 pitanja o sigurnosti - KVIZ (PDF)
- 5 savjeta za sigurno korištenje interneta (PDF)
- 5 savjeta za sigurno korištenje interneta (VIDEO)

http://www.csi.hr/p/materijali-i-savjeti (Pristupljeno 6.11.2018.)

→ Projekt „Safer Internet Centre Croatia: Making internet a good and safe place" (2015-HR-IA-0013) sufinancira Europska unija iz programa Department C - Connecting Europe Facility (CEF). Projekt se provodi pod pokroviteljstvom Innovation and Networks Executive Agency (INEA) na temelju ovlasti delegirane od Europske komisije. Koordinator projekta je Centar za nestalu i zlostavljanu djecu, a partneri su Sveučilište Josipa Jurja Strossmayera, Osijek, Fakultet za odgojne i obrazovne znanosti, Grad Osijek te VIPnet d.o.o. Specifični ciljevi projekta su: daljnji razvoj i promocija centra za podršku i informiranje djece, roditelja, učitelja i drugih koji rade s djecom o boljoj i sigurnijoj upotrebi interneta; poboljšanje *Helpline* usluge za prijavljivanje i pružanje pomoći vezano uz štetne kontakte *(grooming)*, ponašanja (internetsko zlostavljanje-*cyberbullying*) i sadržaje, daljnje održavanje Hotline usluge za primanje i izvještavanje te prikupljanje podataka o protuzakonitom *online* seksualnom zlostavljanju djeteta.

http://cnzd.org/projekti/centar-za-sigurniji-internet (Pristupljeno 6.11.2018.)

→ Projekt „*Prepoznaj rizike digitalnog doba*" je projekt koji je financiralo Ministarstvo socijalne politike i mladih, a kojeg provodi Centar za nestalu i zlostavljanu djecu u partnerstvu s Gradom Osijekom, Sveučilištem Josipa Jurja Strossmayera u Osijeku – Filozofskimfakultetom, Domom za odgoj djece i mladeži Osijek i Dječjim domom Sv. Ana Vinkovci. Specifični ciljevi ovoga projekta bili su uspostava novih alata i mehanizama za prevenciju elektroničkoga nasilja nad i među djecom i mladima; edukacija o elektroničkom nasilju (rano uočavanje i prepoznavanje elektroničkog nasilja, sigurnost na internetu i zaštita osobnih podataka, zaštita prava djece i mladih, *web detektivi*, govor mržnje i *seksting*, simptomatologija žrtve/počinitelja, prevencija i intervencija); podizanje svijesti građana o problemu i prepoznavanju elektroničkog nasilja nad i među djecom i mladima, te poticanje na prijavu istog. Proizišle materijali iz projekta možete pronaći na stranici projekta.

Materijali za edukaciju :

- Prepoznavanje elektroničkog nasilja (PPT)

- *Web detektivi* (PPT)
- Digitalni priručnik o elektroničkom nasilju

Promotivni materijali :

- Plakat *Prepoznaj rizik*
- Letak *Prepoznaj rizike*
- Brošura *Prepoznaj rizike*

http://digitalnirizici.org/materijali/ (Pristupljeno 6.11.2018.)

→ Projekt „*Dvaput razmisli, jednom klikni*" je projekt koji je financiralo Ministarstvo znanosti, obrazovanja i sporta, a kojega provodi Centar za nestalu i zlostavljanu djecu u partnerstvu sa Sveučilištem Josipa Jurja Strossmayera u Osijeku – Fakultetom za odgojne i obrazovne znanosti, Domom za odgoj djece i mladeži Osijek i Centrom za rehabilitaciju „Mala Terezija". Opći cilj projekta „Dvaput razmisli, jednom klikni" je povećati mogućnost djece i mladih da izvan redovitog odgojno-obrazovnog sustava steknu znanja, vještine i usvoje primjerena stajališta o medijskoj pismenost. Razvoj medija čini sve značajnijim pitanja vezana uz utjecaj medija na konzumente medijskih sadržaja, a osobito na djecu, kao najosjetljiviji dio populacije. Sa svrhom ostvarenja općeg cilja, postavljeni su specifični ciljevi projekta: osvješćivanje djece i mladih o nužnosti kritičkog odnosa prema medijskim sadržajima; povećanje medijske pismenosti roditelja djece s teškoćama, asistenata u nastavi te odgajitelja u domovima za nezbrinutu djecu.

Materijali za edukaciju:

- Mediji - *web detektivi* (PPT)
- Edukacijska brošura
- Bonton na internetu (PPT)

Promotivni materijali

- Brošura *Dvaput razmisli*
- Plakat *Dvaput razmisli*

Mobilna aplikacija

- Mobilna aplikacija *Dvaput Razmisli*

Digitalna brošura

- Digitalna brošura *Dvaput razmisli*

http://razmisli.org/materijali-za-strucnjake/ (Pristupljeno 6.11.2018.)

→ Projekt „*Web detektivi"* pokrenut je s ciljem obrazovanja i osposobljavanja djece diljem Republike Hrvatske za usvajanje i razvijanje vještina prepoznavanja neprimjerenih i opasnih medijskih sadržaja kroz održavanje tematskih predavanja i praktičnih radionica s učenicima osnovnoškolske dobi. *Web detektivi* su djeca obučena za prepoznavanje i prijavljivanje neprimjerenih sadržaja na internetu, stoga je namjera projekta u skladu s odredbama o sigurnosti i zaštiti zdravlja odgojno-obrazovnih ustanovama, jer potiče stvaranje uvjeta za zdrav mentalni i fizički razvoj te socijalnu dobrobit učenika, sprječava neprihvatljive i rizične oblike ponašanja, brine se o sigurnosti učenika, omogućava praćenje socijalnih problema i pojava kod učenika i poduzimanja mjera za otklanjanje njihovih uzroka i posljedica, u suradnji s tijelima socijalne skrbi, odnosno drugim nadležnim tijelima, te pospješuje vođenje evidencije o neprihvatljivim oblicima ponašanja učenika, uz mogućnost unaprjeđivanja usluga savjetodavnoga rada s učenicima (Članak 67., Zakon o odgoju i obrazovanju u osnovnoj i srednjoj školi, NN, br 87/08).

http://webdetektivi.org/ (Pristupljeno 6.11.2018.)

2.5. LITERATURA

Beth, H., Jones, B. H., Goyal Chin, A. i Aiken, P. (2014). Risky business: Students and smartphones. *TechTrends*, *58*(6), 73-83.

Davis, K. i James, C. (2013). Tweens' conceptions of privacy online: implications for educators.*Learning, Media and Technology*, *38*(1), 4-25. https://doi.org/10.1080/17439884.2012.658404

DiGi. (2014). *Safety net: Capacity building among Malaysian school children on staying safe online. A national survey report*. Preuzeto s https://digi.cybersafe.my/files/article/CyberSAFE_Survey_Report_2014.pdf, 25.3.2018.

Er, P. H., Cheah, P. K., Moses, P., Chong, C. K. i Ang, B. H. (2017). Awareness of Safe and Responsible Use of ICT Among Students in a Malaysian University. U: G.B. Teh i S.C. Choy (ur.), *Empowering 21st Century Learners Through Holistic and Enterprising Learning*, (str.41-48). Singapore: Springer Nature Pet Ltd. https://doi.org/10.1007/978-981-10-4241-6_5

Gasser, U., Maclay, C. M. i Palfrey Jr. J. G. (2010). Working Towards a Deeper Understanding of Digital Safety for Children and Young People in Developing Nations. *Harvard Law School Public Law & Legal Theory Working Paper Series*, 10-36.

Hall, B. R. (2012). An Ethics Whirlwind: A Perspective of the Digital Lifestyle of Digital Natives and Initial Thoughts on Ethics Education in Technology. *Information Systems Education Journal, 10*(1), 4-12.

Hagen, J. M. i Albrechtsen, E. (2009). Effects on employees' information security abilities by e-learning. *Information Management & Computer Security*, *17*(5), 388-407. https://doi.org/10.1108/09685220911006687

Hrvatska udruga banaka (2017). *Godišnje izvješće Hrvatske udruge banaka o stanju sigurnosti na Internetu u 2016. godini*. Preuzeto s http://www.sigurnostnainternetu.hr/index.php/istrazivanja/item/53-novo-istrazivanje-hub-a-otkriva-hrvati-lezerno-koriste-internet-no-vecina-je-oprezna, 13.5.2018.

Hui, B. i Campbell, R. (2018). Discrepancy between Learning and Practicing Digital Citizenship. *Journal of Academic Ethics, 16*(2), 117–131. https://doi.org/10.1007/s10805-018-9302-9

International Telecommunications Union (2017). *ICT Facts and Figures: The World in 2017*. Geneva, ICT Data and Statistics Division, ITU. Preuzeto s https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx, 15.3.2018.

Jones, B. H., Goyal Chin, A. i Aiken, P. (2014). Risky business: Students and smartphones. *TechTrends*, *58*(6),73-83.

Kim, E. B. (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security*, *22*(1), 115-126. https://doi.org/10.1108/IMCS-01-2013-0005

Lasić-Lazić, J., Špiranec, S., Banek Zorica, M. (2012). Izgubljeni u novim obrazovnim okruženjima-pronađeni u informacijskom obrazovanju. *Medijska istraživanja,* 18(1), 125-142.

Lebek, B., Uffen, J., Neumann, M., Hohler, B. i Breitner, M. H. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, *37*(12), 1049-1092. https://doi.org/10.1108/MRR-04-2013-008

Livingstone, S., Haddon, L., Görzig. A. i Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children. Full findings.* London, EU Kids Online. Preuzeto s http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/D4FullFindings.pdf, 11.2. 2018.

Lomo-David, E., Shannon, L. i Ejimakor, G. (2009). Information systems security and safety measures: The dichotomy between students' familiarity and practice. U: S. Johnson (ur.), *First Annual General Business Conference Conference Proceedings* (str. 268 - 282). Houston: Sam Houston University.

Mensch, S. i Wilkie, L. (2011). Information security activities of college students: An exploratory study. *Acad. Inform. Manage. Sci. Journal, 14,* 91-116.

Robertson, M., Fluck, A. i Thomas, S. (2001). Expert versus novice users: power rules in virtual space. *Australian Educational Researcher*, *28*(1), 147-167. https://doi.org/10.1007/BF03219748

Sharples, M., Graber, R., Harrison, C. i Logan, K. (2009). E-Safety and Web2.0 for children aged 11-16. *Journal of Computer-Assisted Learning*, *25*, 70-84.

Siponen, M.T. (2000). A conceptual foundation for organizational information security awareness, *Information Management & Computer Security*, *8*(1), 31-41. https://doi.org/10.1108/09685220010371394

Thierer, A. (2009). *Parental Controls & Online Child Protection: A Survey of Tools & Methods*. Washington D.C.: The Progress & Freedom Foundation.

Teer, F., Kruck, S., i Kruck, G. (2007). Empirical study of students' computer security practices/ perceptions. *Journal of Computer Information Systems*, *47*(3), 105-110. https://doi.org/10.1080/08874417.2007.11645971

Townsend, A. M. (2010). Mobile communications in the twenty-first century city. U: B. Brown, N. Green, N. i R. Harper, R. (ur.) *Wireless World: Social and Interactional Aspects of the Mobile Age* (str. 62 - 77). New York: Springer.

UNESCO (2015). *World Trends In Freedom of Expression and Media Development: Special Digital Focus 2015*. Preuzeto s http://unesdoc.unesco.org/images/0023/002349/234933e.pdf, 22.2.2018.

Velki, T. ,Šolić, K. i Očević, H. (2014). Development of Users' Information Security Awareness Questionnaire (UISAQ) - Ongoing Work. *Hrvatska udruga za informacijsku i komunikacijsku tehnologiju, elektroniku i mikroelektroniku – MIPRO proceedings,* 1564-1568.

Velki, T., Šolić, K., Gorjanac, V. i Nenadić, K.(2017). Empirical study on the risky behavior and security awareness among secondary school pupils - validation and preliminary results. *Hrvatska udruga za informacijsku i komunikacijsku tehnologiju, elektroniku i mikroelektroniku – MIPRO proceedings,* 1496-1500.

Velki, T., Šolić, K. i Nenadić, K. (2015). Razvoj i validacija Upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava (UZPK). *Psihologijske teme*, *24*(3), 401-424.

Vrana, R. (2013). Online social networks and security of their users: an exploratory study of students at the Faculty of humanities and social sciences Zagreb. U: T. Hunjak, S. Lovrenčić i I. Tomičić (ur.), *Central European Conference on Information and Intelligent Systems* (str. 214 - 221). Varaždin: University of Zagreb Faculty of Organization and Informatics.

Wilcox, H., Bhattacharya, M. i Islam, R. (2014). Social Engineering through Social Media: An Investigation on Enterprise Security. U: L. Batten, G. Li, W. Niu i M. Warren (ur.), *Applications and Techniques in Information Security. ATIS 2014: Communications in Computer and Information Science*, vol.490 (str. 243 - 255). Berlin: Heidelberg Springer.

izv. prof. dr. sc. Tena Velki

Fakultet za odgojne i obrazovne znanosti Osijek

doc. dr. sc. Ksenija Romstein

Fakultet za odgojne i obrazovne znanosti Osijek

3. NACIONALNO ISTRAŽIVANJE RIZIČNOG PONAŠANJA I ZNANJA RAČUNALNIH KORISNIKA

Sažetak

U idućem poglavlju dan je prikaz rezultata nacionalnog istraživanja provedenog na računalnim korisnicima te će se podastrijeti jednostavne strategije zaštite korisnika koji oni mogu primjenjivati sami, iako su prema zakonskim regulativama provajderi interneta dužni zaštiti svoje korisnike, no o tome nemamo dovoljno istraživanja na području EU-a. U istraživanju je sudjelovalo 4859 sudionika (37,5 % muških) iz cijele Hrvatske, podijeljenih u 3 velike skupine; srednjoškolci (n=3250), studenti (n=883) i zaposlenici (n=726). Cilj je bio ispitati znanja i rizična ponašanja korisnika računalnih sustava u cijeloj Republici Hrvatskoj, uzimajući pri tom u obzir dobne i spolne razlike. Provjereno je i stvarno ponašanje odavanja zaporke korisnika računalnih sustava. Također je utvrđena povezanost informacijskoga znanja s rizičnim ponašanjem računalnih korisnika. Rezultati istraživanja su pokazali kako jako puno sudionika (31% - 54,2%) dobrovoljno odaje svoju zaporku te su studentiu tom pogledu najrizičnija skupina. Odrasli zaposlenici pokazuju najviše rizičnog ponašanja vezanog uz korištenje informacijskih sustava, ali istovremeno i najveći stupanj znanja. Iza njih slijede studenti, a na kraju srednjoškolci s najnižim stupanjem znanja, ali i rizičnoga ponašanja. Općenito je utvrđeno da osobe s višom razinom znanja o informacijskoj sigurnosti pokazuju i viši stupanj rizičnih online ponašanja. Dobiveni podatci su u skladu s istraživanjima koja su provedena u zemljama EU-a u kojima je nađena povezanost rizičnih

ponašanja i kronološke dobi korisnika te rizičnih ponašanja i količine vremena provedene na internetu. Tako djeca i mladi koji provode više vremena na internetu češće manifestiraju rizična ponašanja kao npr. odavanje svojih osobnih podataka nepoznatim osobama, prihvaćanje prijateljstava i poruka od nepoznatih osoba, sve do sastajanja offline s online prijateljima koje nisu prethodno upoznali u stvarnom životu. Što se tiče odraslih, istraživanja provedena zemljama EU-a nešto su manje opsežna i govore uglavnom o korištenju alata kao što su net-banking ili nadgledanje korištenja interneta djece, nedostaju podatci za populaciju odraslih, što se djelomice tumači opadanjem rizika s porastom kronološke dobi, no ta pretpostavka nije do kraja potvrđena. Ukratko, ponašanja korisnika interneta ovise o trima čimbenicima, a to su kulturalni kontekst, zakonska regulativa i odgojno-obrazovni kontekst, što treba uvažiti prilikom provođenja budućih istraživanja, kao i kreiranja smjernica za zaštitu internetskih korisnika od najmlađe dobi.

3.1. UVOD

Sveprisutnost interneta u svakodnevnom životu ljudi dovela je do pojave da virtualni svijet postaje sve više dio stvarnog realnog svijeta, odnosno gube se jasne granice između virtualnog i stvarnog svijeta. Internet sve više obuhvaća postojeći realni svijet te kao takav ulazi u sva područja života čovjeka, gdje današnji suvremeni život postaje nezamisliv bez svakodnevne upotrebe interneta. Upravo ova promjena suvremenog društva gdje se aktivnosti sele iz realnog u virtualni svijet, omogućuje i ubrzani razvoj socijalnog inženjeringa, odnosno razvoj internetskih prijevara koje se ciljano usmjeravaju na lakovjernog korisnika (Haley, 2011; Mitnick, Simon i Wozniak, 2002; Selmar i Tibert, 2018). Početno, na prvu beznačajno, odavanje manjeg broja osobnih podataka npr. pri instalaciji manjih aplikacija, korištenjem društvenih mreža, online kupnji kino ulaznica i sl. može u konačnici dovesti do materijalnih gubitaka, ali i dijelom gubitka privatnosti. Korisnici koji su neoprezni, nesmotreni i općenito nesvjesni potencijalnog rizika predstavljaju najveći problem pri osiguravanju informacijske sigurnosti. Niz istraživanja tijekom posljednja dva desetljeća jasno pokazuje kako je sam računalni korisnik, odnosno ljudska komponenta najslabija karika po pitanju informacijske sigurnosti (Lukasik, 2011; Sasse, Brostoffand i Weirich, 2001). Korisnici informacijskih sustava svojim nepromišljenim i rizičnim ponašanjem mogu značajno utjecati na cijeli sustav informacijske sigurnosti. Važnost znanja, ponašanja i svijesti o pitanjima sigurnosti informacijskih i privatnih podataka među korisnicima interneta prvo su prepoznali mrežni administratori i stručnjaci za sigurnost, a tek nakon toga ovom se problematikom počinju baviti znanstvenici. Međutim još je uvijek relativno malo znanstvenih istraživanja u ovom području (Crossler i sur., 2013; Kwang i Choo, 2011), a većina njih se uglavnom bavila pitanjem kvalitete i snage zaporke korisnika računalnih sustava (Dell'Amico, Michiardi i Roudier, 2010; Kelley i sur., 2012; Voyiatzis, Fidas, Serpanos i Avouris, 2011; Wanli, Campbell, Tran i Kleeman, 2010). Tako je npr. jedno novije istraživanje pokazalo kako većina korisnika jačinu i kvalitetu svoje zaporke procjenjuje kao prosječnu, a samo 13,8% korisnika kao lošu (*Šolić, Očevćić i Blažević, 2015*), no postavlja se pitanje kako bi stručnjaci procijenili njihove zaporke. Nadalje, isti korisnici (53,4%) preferiraju koristiti istu zaporku za pristup većini korištenih informacijskih sustava što uvelike narušava informacijsku sigurnost. Drugim riječima, percepcija sigurnosti i rizika je individualna. O osobnom, individualnom tumačenju sigurnosti (*safety/security*) i rizika govori i Europska agencija za informacijsku sigurnost (ENISA, 2014) te pojašnjava kako su osobna ponašanja ključna za pitanje sigurnosti pojedinca, a i interneta općenito.

Literatura na području *online* sigurnosti uglavnom ne daje veliku važnost istraživanjima rizičnih ponašanja odraslih korisnika, već se uglavnom fokusira na djecu i maloljetnike, koje vidi kao izrazito vulnerabilnu populaciju u odnosu na virtualni svijet. Izostajanje propitivanja rizičnih ponašanja odraslih vodi prema simplificiranom pristupu sistemske perspektive prevencije opasnosti kojima djeca mogu biti izložena. Naime, istraživanje ENISA-e (2014) pokazuje kako su *online* ponašanja roditelja i djece slična te se može zaključiti kako se *online* ponašanja uče, tj. *online* ponašanja odraslih mogu biti model ponašanja djeci. Prvi veći pomaci napravljeni su razvojem upitnika koji mjere znanja i ponašanja korisnika informacijskih sustava, a znanstvenici iz Republike Hrvatske su bili među prvima u svijetu koji su se počeli baviti razvojem *Upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava* (Velki, Šolić i Očevćić, 2014). Prva istraživanja na punoljetnim zaposlenicima su otkrila zabrinjavajuće podatke. Čak oko 30% zaposlenika dobrovoljno je otkrilo svoju zaporku istraživačima koju koriste za službenu e-poštu (Šolić, Velki i Galba, 2015). Još više zabrinjava podatak dobiven za srednjoškolce od kojih je čak 78% otkrilo svoju zaporku koju koriste za privatnu e-poštu, što je statistički značajno više nego kod zaposlenika (Velki, Šolić, Gorjanac i Nenadić, 2017). Upravo problem davanja zaporke i osobnih podataka ENISA (2014) navodi kao vodeći izazov u informatičkom opismenjavanju jer je sigurnost osobnih podataka (uključujući i zaporku) jedna od prvih tema u programima informatike, pa nije do kraja jasno otkuda ova vrsta rizičnog ponašanja iako se na formalnoj razini o tome razgovara s korisnicima već u školskim klupama. Zaposlenici koji rade u privatnom sektoru češće su odavali svoju zaporku od zaposlenika koji rade u državnom sektoru. Zaposlenici s višim stupnjem obrazovanja (završenim fakultetom) u odnosu na zaposlenike s nižim stupnjem obrazovanja (završena srednja škola) bili su pouzdaniji i rjeđe su otkrivali zaporku. Općenito osobe koje nisu otkrile svoju zaporku pokazale su bolje znanje o informacijskoj sigurnosti (npr. prave kopije važnih dokumenata, provjeravaju antivirusnim programom vanjsku memoriju i sl.) i manje rizičnog ponašanja (npr. održavaju zaštitu kućnog računala, ne govore drugima svoje PIN brojeve i zaporke i sl.) (Šolić, Velki i Galba, 2015), dok su studenti koji nisu odali svoju zaporku pokazivali manje rizičnog ponašanja korištenjem računala, ali podjednaku razinu znanja kao i studenti koji su odali svoju zaporku (Velki, Šolić i Nenadić, 2015). U odnosu na odrasle zaposlenike, srednjoškolci su pokazali rizičnije *online* ponašanje (npr. posuđuju svoje pristupne podatke prijateljima i rođacima, šalju lančane poruke, odgovaraju na e-poštu nepoznatih osoba i sl.), problematičniju *online* komunikaciju (npr. dopisivanje e-poštom s nepoznatim osobama, odavanje osobnih podataka putem društvenih mreža i sl.) te su slabije pohranjivali računalne podatke, no bili su bolji u održavanju računala i po pita-

nju uvjerenja o informacijskoj sigurnosti podataka tj. mogućnosti krađe i zlouporabe informacijskih podataka gdje su pokazali veću svjesnost vezano uz ovu problematiku (Velki i sur., 2017). Žene (studentice i odrasle zaposlenice) su u odnosu na muškarce opreznije i skeptičnije u otkrivanju privatnih podataka putem *online* sustava (Šolić, Velki i Galba, 2015), što vrijedi i za srednjoškolce (Velki i sur., 2017). Stariji zaposlenici u odnosu na mlađe (mlađe od 30 godina) pokazali su veće ukupno znanje po pitanju informacijske sigurnosti i manje rizičnog ponašanja. (Šolić, Velki i Galba, 2015), dok su studenti u odnosu na zaposlenike bolje održavali računala, ali su istovremeno bili neoprezni i prakticirali nesigurniji tip *online* komunikacije (Velki, Šolić i Nenadić, 2015). I za srednjoškolce i za odrasle sudionike istraživanja dobiven je statistički značajna povezanost između skala znanja o informacijskoj sigurnosti i skala rizičnog ponašanja korisnika računala pri čemu osobe koje posjeduju viša znanja i svjesnije su potencijalne opasnosti, ujedno se i rizičnije ponašaju pri korištenju informacijskih sustava (Velki i sur., 2017). Također se i neka prijašnja istraživanja pokazala da je sama svjesnost i znanje o informacijskoj sigurnosti nedovoljno da se osoba ponaša u skladu s tim, čak i među vrlo obrazovanim sveučilišnim profesorima (Šolić i Ilakovovac, 2009; Šolić, Ilakovac, Marušić i Marušić, 2009).

Što se tiče istraživanja u zemljama EU-a, ona su uglavnom usmjerena na identifikaciju *online* rizika za djecu i mlade, dok se u odnosu na odraslu dob (nakon 21. godine života) vrlo rijetko pojavljuju. Čini se kako se interes za odrasle, kao korisnike interneta, javlja uglavnom u kontekstu zaštite djece, dok se odrasla dob ne vidi kao posebno osjetljiva dob za rizična *online* ponašanja. ENISA (2014) u svojemu istraživanju pronalazi kako rizici opadaju s kronološkom dobi, no to nije do kraja moguće potvrditi iz nekoliko razloga: prvi je temeljenje istraživanja na samoprocjenama korisnika tj. izostanak softvera koji bi prikupio i izračunao podatke o rizičnim ponašanjima korisnika neovisno o njihovoj procjeni vlastita ponašanja u *online* svijetu. Nadalje, odrasli su skloniji socijalnom konformizmu, pa ako i prakticiraju rizična ponašanja, manja je vjerojatnost da će to otvoreno i priznati. Naposljetku, moguće je da su se odrasli tijekom korištenja interneta susreli sa sadržajima koji su ih uznemirili, no tijekom vremena su razvili strategije nošenja s rizicima i nelagodom, pa lakše mogu prepoznati potencijalne rizične situacije, što djeci i mladima uglavnom nedostaje. Odnosno, odrasli imaju iskustvo koje im može olakšati učinkovitije snalaženje u online svijetu. Upravo prepoznavanje rizičnih situacija je iznimno bitno gledište *online* sigurnosti, jer se sigurnost nikada ne može u potpunosti postići, ali je moguće prepoznavanje rizika i reduciranje njihovih učinaka ako se na vrijeme prepoznaju (ENISA, 2014). Stoga je prikupljanje podataka od samih korisnika prvi korak u razvijanju algoritama *online* sigurnosti, što je bila i glavna svrha ovog istraživanja.

Cilj: Ispitati osnovne karakteristike računalnih korisnika i međusobno usporediti rezultate za različite korisnike.

1.) Ispitati dobne razlike u znanju i rizičnom ponašanju računalnih korisnika (srednjoškolci, studenti i odrasli djelatnici).
2.) Ispitati spolne razlike u znanju i rizičnom ponašanju računalnih korisnika.
3.) Ispitati razlike u znanju i rizičnom ponašanju računalnih korisnika u odnosu na odavanje zaporke.
4.) Ispitati odnos između znanja o informacijskoj sigurnosti i rizičnog ponašanja računalnih korisnika.

3.2. METODA

3.2.1. SUDIONICI

U istraživanju je ukupno sudjelovalo 4859 sudionika (37,5 % muških) iz cijele RepublikeHrvatske. Raspon dobi se kretao od 14 do 65 (M=20,78, SD=9,52), prosječna dob srednjoškolaca bila je M=16,24 (SD=1,08), prosječna dob studenata M=21,93 (SD=4,29) te prosječna dob odraslih djelatnika (odrasle zaposlene osobe) M=39,68 (SD=11,26). U Tablici 1. je prikazana je raspodjela sudionika prema spolu, a u Tablici 2. i na Slici 1. rasprostranjenost prema regijama iz koje dolaze sudionici.

Tablica 1. Raspodjela sudionika po spolu

			muško		**žensko**	
Sudionici	**N**	**%**	**N**	**%**	**N**	**%**
srednjoškolci	3250	66,9	1317	40,5	1933	59,5
studenti	883	18,2	216	24,5	667	75,5
djelatnici	726	14,9	287	39,5	439	60,5
Ukupno	**4859**	**100,0**	**1820**	**37,5**	**3039**	**62,5**

Tablica 2. Rasprostranjenost sudionika prema regijama iz kojih dolaze

Sudionici	Srednjoškolci		Studenti		Djelatnici		UKUPNO	
Regija	**N**	**%**	**N**	**%**	**N**	**%**	**N**	**%**
Istočna Hrvatska (Sveučilište u Osijeku)	775	23,8	695	78,7	220	30,3	1690	34,8
Sjeverozapadna i središnja Hrvatska (Sveučilište u Zagrebu)	1632	5,2	113	12,8	319	43,9	2064	42,5
Sjeverni Jadran i Lika (Sveučilište u Rijeci)	207	6,4	35	4,0	122	16,8	364	7,5
Srednji i južni Jadran (Sveučilište u Zadru)	636	19,6	40	4,5	65	9,0	741	15,2
Ukupno	**3250**	**100,0**	**883**	**100,0**	**726**	**100,0**	**4859**	**100,00**

Slika 1.
Rasprostranjenost sudionika prema regijama Republike Hrvatske iz kojih dolaze

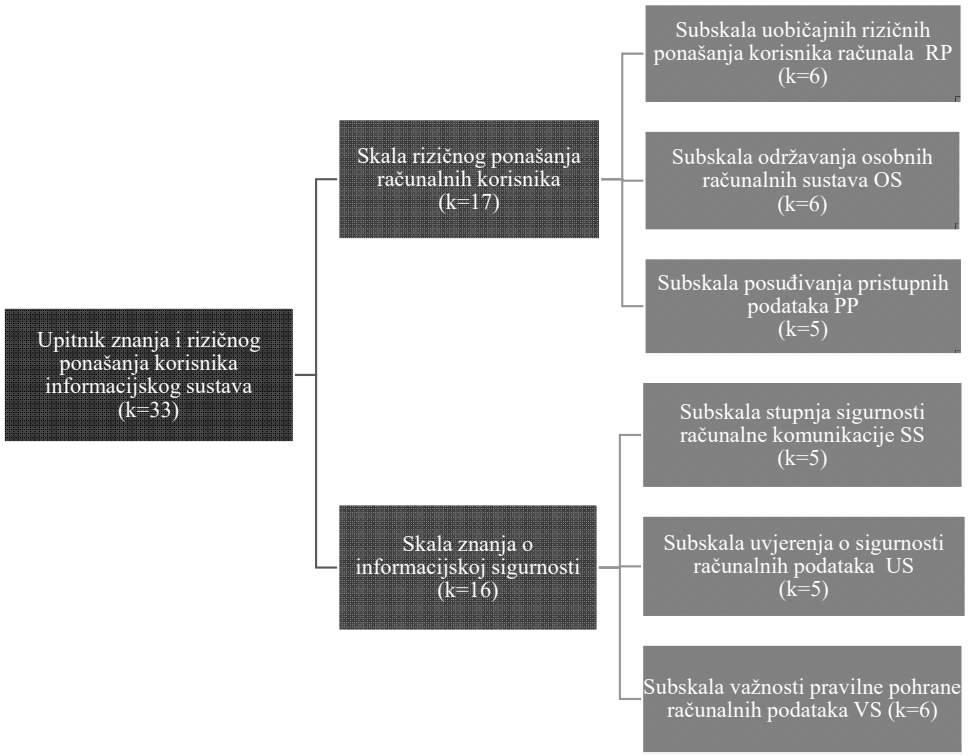
3.2.2. INSTRUMENTI

Upitnik znanja i rizičnog ponašanja korisnika informacijskog sustava (UZPK; Velki i Šolić, 2014; prema Velki, Šolić i Nenadić, 2015)

U istraživanju je korišten *Upitnik znanja i rizičnog ponašanja korisnika informacijskog sustava* koji ispituje rizična ponašanja i znanja računalnih korisnika

te je namijenjen za odrasle osobe. Upitnik se sastoji od općih demografskih pitanja (spol, dob, mjesto stanovanja i sl.), testnog pitanja o odavanju zaporke te dvije glavne skale: Skala rizičnog ponašanja računalnih korisnika (k=17) i Skala znanja o informacijskoj sigurnosti (k=16). Skala rizičnog ponašanja računalnih korisnika dijeli se u tri subskale, pri čemu Subskala uobičajenih rizičnih ponašanja računalnih korisnika - RP (k=6) mjeri različita rizična ponašanja (npr. *Otvarate, bez provjere, priloge od nepoznatih pošiljatelja)*, Subskala održavanja osobnih računalnih sustava – OS (k=6) mjeri učestalost i kvalitetu održavanja osobnih računalnih sustava (npr. *Koristite različite lozinke za različite sustave, npr. za Facebook jedna, za e-poštu druga, za poslovni sustav treća lozinka, itd.),* a Subskala posuđivanja pristupnih podakata (k=5) mjeri učestalost odavanja različitih pristupnih podataka (npr. *Posuđujete svojim prijateljima, rođacima, poznanicima svoje privatne pristupne podatke za pristup osobnoj/privatnoj adresi e-pošte*). Drugi dio upitnika, koji mjeri znanje o informacijskoj sigurnosti, također se sastoji od 3 subskale. Subskala stupnja sigurnosti računalne komunikacije – SS (k=5) mjeri procjenu stupnja informacijske sigurnosti korisnika (npr. Što mislite koliko je sigurna komunikacija putem društvenih mreža (npr. Facebook, Twitter), Subskala uvjerenja o sigurnosti računalnih podataka – US (k=5) mjeri stupanj uvjerenja korisnika o informacijskoj sigurnosti podataka (npr. *Koliko ste uvjereni da postoji realna opasnost da će vam netko ukrasti privatne podatke s vašeg kućnog računala*) te posljednja Subskala važnosti pravilne pohrane računalnih podataka – VS (k=6) procjenjuje stupanj važnosti pravilnog čuvanja računalnih podataka (npr. *Prema vašem mišljenju koliko je važno provjeriti tuđi USB memorijski štapić od virusa prije učitavanja podataka*). Pouzdanost UZPK-a za studente se kretala između Cronbach α = 0,69 – 0,84, a za odrasle djelatnike Cronbach α = 0,67 - 0,88.

Za potrebe istraživanja napravljena je i validirana prilagođena inačica za srednjoškolsku populaciju (Velki i Šolić, 2016; prema Velki, Šolić, Gorjanac i Nenadić, 2017). Prilagodba se sastojala u sadržaju pojedinih čestica gdje su pitanja oblikovana da ispituju korištenje računala na poslu/fakultetu prilagođena za ispitivanje korištenja računala u školi. Dobivena je paralelna inačica UZPK-a koja se sastojala od identičnih skala i subskala. Pouzdanost UZPK-a za srednjoškolce se kretala između Cronbach α = 0,66 – 0,84.



Slika 2.
Prikaz skala i subskala Upitnik znanja i rizičnog ponašanja korisnika informacijskog sustava

3.2.3. POSTUPAK

Istraživanje je provedeno *online*, u potpunosti anonimno, tijekom jedne godine. Ustanove (škole, fakulteti i tvrtke) prvo su kontaktirane telefonski i elektroničkom poštom, a koje su pristale na suradnju dobile su i pismenu zamolbu s detaljnim objašnjenjem svrhe istraživanja, kao i uputama o provođenju istraživanja. Nakon toga su ima poslani linkovi putem kojeg su mogli pristupiti popunjavanju upitnika. Svaka ustanova je dobila svoju poveznicu. Poveznicesu bile aktivne između 3 i 6 mjeseci, a podaci su se automatski upisivali u bazu podataka za svaku ustanovu. Po završetku istraživanja svaka ustanova koja je sudjelovala u istraživanju dobila je podatke za svoje sudionike i njihovu usporedbu u odnosu na ostale sudionike u RepubliciHrvatskoj.

3.3. REZULTATI I RASPRAVA

Tablica 3. Prikaz deskriptivnih podataka za skale i subskale UZPK-a (svi sudionici, N=4859)

UZPK skale i subskale	raspon	Min	Max	M	SD	varijanca	indeks asimetričnosti	indeks spljoštenosti
Skala rizičnog ponašanja računalnih korisnika	4,00	1,00	5,00	4,00	0,42	0,17	-0,73	1,69
Skala znanja o informacijskoj sigurnosti	4,00	1,00	5,00	3,07	0,53	0,28	0,08	0,69
Subskala posuđivanja pristupnih podataka	4,00	1,00	5,00	4,66	0,49	0,24	-2,98	3,38
Subskala održavanja osobnih računalnih sustava	4,00	1,00	5,00	3,27	0,83	0,69	-0,32	-0,01
Subskala uobičajenih rizičnih ponašanja korisnika računala	4,00	1,00	5,00	4,16	0,59	0,35	-1,32	3,22
Subskala stupnja sigurnosti računalne komunikacije	4,00	1,00	5,00	2,93	0,82	0,67	0,34	0,05
Subskala uvjerenja o sigurnosti računalnih podataka	4,00	1,00	5,00	2,32	0,87	0,76	0,71	0,18
Subskala važnosti pravilne pohrane računalnih podataka	4,00	1,00	5,00	3,83	0,78	0,61	-1,17	1,87

U Tablici 3. prikazani su deskriptivni podatci za sve skale i subskale UZPK-a primijenjene na nacionalnom uzorku. Sve skale i subskale pokazuju puni raspon odgovora, odnosno zadovoljavajuću osjetljivost mjernog instrumenta. Nadalje, indeksi asimetrije ne pokazuju značajna odstupanja (< +/- 4) što upućuje na normalnost distribucije i mogućnost primjene parametrijske statistike u daljnjim analizama podataka.

Tablica 4. Prikaz odavanja zaporke za različite sudionike (svi sudionici, N=4662)

zaporka	srednjoškolci		studenti		djelatnici		ukupno	
	N	%	N	%	N	%	N	%
ne	2244	69,0	404	45,8	313	59,2	2961	63,5
da	1006	31,0	479	54,2	216	40,8	1701	36,5
Ukupno	**3250**	**10,0**	**883**	**100,0**	**529**	**100,0**	**4662**	**100,0**

* napomena: 197 djelatnika nije imalo pitanje o zaporci zbog sigurnosne politike tvrtke

Rezultati istraživanja (Tablica 4.) pokazuju kako između 31% i 54,2% sudionika istraživanja dobrovoljno daje svoju zaporku koje koriste za elektroničku poštu što upućuje na zabrinjavajući činjenicu o odavanju osobnih podatka pri korištenju interneta. Prijašnja istraživanja pokazala su kako nešto manji broj zaposlenika (oko 30%), ali puno veći broj srednjoškolaca (oko 78%) odaju svoju zaporku za e-poštu (Šolić, Velki i Galba, 2015; Velki i sur., 2017). ENISA (2014) istraživanje pokazuje kako je odavanje zaporke povezano s uporabom interneta na nacionalnoj razini, odnosno, u državama EU-a u kojima se internet koristi u većem postotku (primjerice Danska, Švedska) odrasli manje daju zaporke drugima, ali su i manje zabrinuti za *online* sigurnost djece i mladih. S druge strane, u zemljama u kojima se internet manje koristi (npr. Grčka, Španjolska, Portugal) davanje zaporke je češće, ali je i zabrinutost za *online* sigurnost djece veća. Razlog tomu može biti nedostatno poznavanje interneta, *online* rizika i strategija prevencije, tj. korisnici koji manje poznaju internet zabrinutiji su za sigurnost djece, dok u isto vrijeme oni sami manifestiraju rizična ponašanja. Z-testom proporcija utvrđene su i statističke značajne razlike u odavanju zaporka za različite skupine sudionika istraživanja. Srednjoškolci su statistički značajno najmanje skloni odavanju zaporke ($z=12,7$, $p<0,01$ u odnosu na studente, te $z=4,9$, $p<0,01$ u odnosu na zaposlenike) što djelomično može biti odraz odrastanja u virtualnom svijetu, odnosno informacijske pismenosti koju su usvojili kroz odgoj i/ili školovanje. Iako se broj odraslih koji odaju zaporku nešto povećao na temelju podataka prijašnjih istraživanja (Šolić, Velki i Galba, 2015; Velki i sur., 2017) i ukazuje na trend sve intenzivnijeg korištenja informacijskih sustava, pa posljedično tome i potencijalnih opasnosti koje donose *online* sustavi, za mlađe sudionike je primijećen pozitivan trend. Moguće je da su zbog školovanja, posebice u sklopu satova informatike, srednjoškolci postali svjesniji zlouporabe privatnih podatka koji dobrovoljno odaju, pa se imaju potrebu i želju bolje zaštiti, odnosno sačuvati svoju privatnost. Također je moguće zbog velike uporabe, a posebice zlouporabe društvenih mreža da su srednjoškolci upravo skupina koja je tim promjenama najpogođenija i vrlo je vjerojatno da imaju i izravnog iskustva u vidu doživljajna ili činjenja elektroničkog nasilja, što je i pokazano u nekim istraživanjima (Velki

i sur., 2017), pa su stoga postali oprezniji pri odavanju osobnih podataka. Što se tiče *online* rizičnih ponašanja djece i mladih u zemljama EU-a, Livingstone i Haddon (2009) pronalaze kako u prosjeku 75% djece u dobi od 7 do 18 godina koriste internet na dnevnoj bazi, a rizična ponašanja koja pritom prakticiraju su davanje osobnih podataka i zaporke drugim (nepoznatim) osobama, prihvaćanje prijateljstava i poruka od nepoznatih osoba, te nalaženje licem-u-lice s *online* prijateljima koje prethodno nisu upoznali, što je ujedno i najveći rizik za djetetovu sigurnost. Davanje zaporke i osobnih podataka je najučestalije i ono se penje i do 50% u državama s niskom razinom korištenja interneta (i informatičke pismenosti), dok su nalaženja licem-u-lice najrjeđa i o njima zapravo ne postoje egzaktni podatci, no autori procjenjuju da se oko 10% djece i mladih odlučuje na taj korak.

Djelatnici različitih poduzeća statistički značajno manje odaju zaporku u odnosu na studente ($z=4,1$, $p<0,01$) što nas vodi k zaključku da su studenti najrizičnija skupina po odavanju zaporke u ovom istraživanju. Ovaj rezultat se može objasniti paradoksom obrazovanja. Iako su studenti u prosjeku najobrazovanija skupina sudionika, znanje o informacijskoj sigurnosti i općenito informacijska pismenost za njih ne predstavlja čimbenik zaštite, već rizični čimbenik u kontekstu informacijske sigurnosti. Upravo posjedovanje i svjesnost da imaju znanja o zaštiti podataka u informacijskim sustavima čini ih sklonijima odavanju vlastite zaporke jer smatraju da se njima ne može dogoditi krađa podataka putem informacijskih sustava baš zato što oni o tome puno znaju, što su pokazala i prijašnja istraživanja uključujući i visoko obrazovane sudionike (Šolić i Ilakovovac, 2009; Šolić i sur,, 2009). Međutim, upravo ta lažno stvorena sigurnost čini ih najrizičnijom skupinom. Drugi mogući razlog je testiranje vlastitih mogućnosti nošenja s rizicima, tj. psihološki čimbenici, koji se u literaturi ne spominju. Ipak, Starčević (2015) govori kako je kod korištenja interneta ključan psihološki čimbenik tj. osobine ličnosti korisnika koje određuju njegovo ponašanje, što je katkada teško mijenjati edukacijom.

3.3.1. GLAVNA ANALIZA PODATAKA: MULTIVARIJANTNA ANALIZA VARIJANCE

Kako bi se ispitali učinci spola, dobi i odavanje zaporke na sve tri skupine sudionika istraživanja (srednjoškolci, studenti i zaposlenici) provedena je multivarijatna analiza varijance (MANOVA). U Tablici 5. prikazani su rezultati MANOVA koji nam govore postoje li značajne dobne, spolne te razlike u odavanju zaporke za sudionike istraživanja, odnosno razlikuju li se npr. muškarci od žena u rizičnom

online ponašanju (što je prva skala UZPK-a). Za sve dobivene značajne razlike (red u tablici označen **) dana su detaljnija objašnjenja u nastavku teksta.

Tablica 5. Rezultati 3 x 2 x 2 MANOVA (dob x spol x zaporka) za skale i subskale UZPK-a (N = 4859)

	Pillai's trace	Wilks' Lambda	F	ss1	ss2
Dob	0,07	0,93	20,80**	2	4857
Spol	0,13	0,87	88,02**	1	4858
Zaporka	0,22	0,78	72,12**	1	4858
Dob x Spol	0,01	0,99	2,73**	5	4854
Dob x Zaporka	0,01	0,99	2,35**	5	4854
Spol x Zaporka	0,17	0,84	52,99**	3	4856
Dob x Spol x Zaporka	0,01	0,99	2,29**	11	4848

*p < 0,05; **p < 0,01; ss – stupnjevi slobode

Multivarijantna analiza varijance (Tablica 5.) pokazala je postojanje dobnih, spolnih i razlika u odavanju zaporke za skale i subskale UZPK-a, kao i postojanje statistički značajnih interakcijskih učinaka. Daljnjim *post-hoc* analizama (*Hochbergovim post-hoc testom*) provjeravani su glavni učinci za sve skale i subskale UZPK-a, kao i svi interakcijski učinci(npr. starije žene koje ne odaju svoju zaporku u odnosu na mlađe muškarce koji odaju zaporku). Veći rezultati na skali i subskalama ponašanja ukazuju na viši stupanj rizičnog ponašanja računalnih korisnika, dok veći rezultati na skali i subskalama znanja ukazuju na viši stupanj znanja računalnih korisnika.

3.3.1.1. Dobne razlike u znanju i rizičnom ponašanju računalnih korisnika

U provedenom istraživanju sudionici su prema dobi bili podijeljeni u tri skupine, učenici srednjih škola, studenti i odrasle zaposlene osobe. Cilj istraživanja bio je i provjeriti razlikuju li se ove tri dobne skupine međusobno rizičnom *online* ponašanju te u svojem znanju o informacijskoj sigurnosti. Kako je dobiven značajni glavni pokazatelj dobi (MANOVA, Tablica 5.) dodatnim analizama utvrđene su dobne razlike za svaku skalu i subskalu UZPK-a.

Tablica 6. Prikaz dobnih razlika za pojedine skale i subskale UZPK-a

UZPK	Dob	M	SD	$F_{(2,4857)}$
Skala rizičnog ponašanja računalnih korisnika	Srednjoškolci	3,96	0,42	54,96**
	Studenti	4,06	0,42	
	Odrasli zaposlenici	4,11	0,39	
Skala znanja o informacijskog sigurnosti	Srednjoškolci	3,04	0,53	31,03**
	Studenti	3,08	0,52	
	Odrasli zaposlenici	3,19	0,49	
Subskala posuđivanja pristupnih podataka	Srednjoškolci	4,67	0,50	5,66**
	Studenti	4,61	0,52	
	Odrasli zaposlenici	4,70	0,42	
Subskala održavanja osobnih računalnih sustava	Srednjoškolci	3,22	0,82	37,15**
	Studenti	3,45	0,78	
	Odrasli zaposlenici	3,33	0,87	
Subskala uobičajenih rizičnih ponašanja korisnika računala	Srednjoškolci	4,10	0,61	47,44**
	Studenti	4,21	0,53	
	Odrasli zaposlenici	4,39	0,51	
Subskala stupnja sigurnosti računalne komunikacije	Srednjoškolci	2,84	0,78	52,91**
	Studenti	3,03	0,82	
	Odrasli zaposlenici	3,21	0,87	
Subskala uvjerenja o sigurnosti računalnih podataka	Srednjoškolci	2,34	0,93	1,61
	Studenti	2,33	0,78	
	Odrasli zaposlenici	2,22	0,72	
Subskala važnosti pravilne pohrane računalnih podataka	Srednjoškolci	3,80	0,83	23,04**
	Studenti	3,78	0,69	
	Odrasli zaposlenici	4,02	0,59	

*p < 0,05; **p < 0,01

Hochbergovim post-hocom testom utvrđene su statistički značajne razlike za skale i subskale UZPK-a. Odrasli zaposlenici pokazuju najviše rizičnog ponašanja vezanog uz korištenje informacijskih sustava, ali istovremeno i najviši stupanj znanja. Iza njih slijede studenti, a na kraju srednjoškolci s najmanjim stupanjem znanja, ali i rizičnog ponašanja. Iako je očekivano da će studenti pokazati najviši stupanj znanja, ali i rizičnog ponašanja, što je u skladu s njihovim odavanjem zaporke, ali i nekim prijašnjim istraživanjima (Velki, Šolić i Nenadić, 2015; Velki i sur., 2017), moguće je da su zapravo samo oni zaposlenici koji posjeduju visoku informacijsku pismenost i često se služe računalom na radnom mjestu popunili tražene upitnike dok ostali sudionici, koji su manje informacijski pismeni, nisu ni pristupili popunjavanju upitnika, čemu u prilog idu i prijašnja istraživanja na visoko obrazovanim institucijama.

Gledajući rezultate post-hoc analize za različite subskale UZPK-a vidimo slične obrasce ponašanja. Na subskali posuđivanja pristupnih podataka srednjoškolci i zaposlenici statistički značajno češće posuđuju pristupne podatke za razliku od studenata koji su očito prijašnjim online iskustvom, ali i razinom obrazovanja postali svjesniji mogućih rizika pri odavanju privatnih podataka. Na subskali održavanja računalnih sustava srednjoškolci su se pokazali kao najbolji, zatim zaposlenici, dok studenti najmanje vode računa o održavanju računala kojim se svakodnevno koriste. Za srednjoškolce je održavanje računala sastavni dio školskog gradiva pa ne čudi da o tome pokazuju najviša znanja, ali i kao najmlađa generacija koja je odrasla uz virtualni svijet, odnosno niz različitih informacijskih sustava, za njih je ova praksa održavanja sustava svakodnevna i uobičajena pojava, a ne nešto što se dodatno mora savladati i naučiti kao kod starijih sudionika. Na subskali uobičajenih rizičnih ponašanja korisnika računala najviše rizičnog ponašanja pokazali su zaposlenici, zatim studenti, a najmanje srednjoškolci. Iako bi se možda očekivalo da srednjoškolci, odnosno adolescenti, zbog razvojne životne dobi, pokazuju najviše rizičnih ponašanja vezanih uz informacijske sustave, upravo su oni skupina koja je od najranijih dana upoznata s različitim informacijskim sustavima (npr. pametni telefoni, tableti, prijenosna računala) i ima najviše izravnog iskustva u korištenju različitih aplikacija (npr. društvenih mreža, aplikacija za komunikaciju i sl.) kao i drugih programa (npr. različitih antivirusnih programa i dr.) što ujedno predstavlja sklop specifičnih znanja stečenih na temelju svakodnevne prakse i omogućuje im bolje snalaženje u svakodnevnom radu s informacijskim sustavima, za razliku od najstarije dobne skupine koja ova znanja stječu tijekom rada ili se moraju dodatno formalno obrazovati da bi se znali pravilno služiti informacijskim sustavima. Nisu na svim subskalama znanja dobiveni statistički značajne razlike. Na subskali uvjerenja o sigurnosti računalnih podataka nisu dobivene dobne razlike, što znači da su bez obzira na dob sudionici podjednako uvjereni da im treće osobe mogu ukrasti privatne podatke s računala ili mobitela. Subskala stupnja sigurnosti računalne komunikacije pokazala je isti obrazac, odnosno najviši stupanj znanja vezano uz sigurnost računalne komunikacije pokazali su zaposlenici, zatim studenti, a najmanje srednjoškolci. Srednjoškolci su skupina koja je najviše izložena komunikaciji u virtualnom svijetu, posebice putem društvenih mreža, pa s obzirom na količinu vremena koju provodi *online* s vršnjacima ne čudi da su najmanje svjesni mogućih posljedica ovakvog tipa komunikacije (npr. krađa podataka, presretanje informacija koje proslježuju jedni drugima i sl.). Što se tiče važnosti pravilne pohrane podataka zaposlenici u odnosu i na studente i na srednjoškolce pokazuju višu razinu znanja, što je i očekivano. Zaposlenicima je pravilna pohrana nužna za svakodnevno obavljanje posla i vjerojatno iz toga proizlazi i shvaćanje koliko je važno imati sačuvane podatke s kojim se svakodnevno radi.

Zanimljivu činjenicu o rizičnom *online* ponašanju korisnika pronalazi ENISA (2014). Naime, savjete o smanjenju rizika i povećanju sigurnosti korisnici uglavnom traže upravo na internetu pri čemu nerijetko krše uobičajena pravila zaštite kao što su odavanje zaporke ili adrese. Također, prema njihovu istraživanju, jednu od najnižih razina informatičko-komunikacijskih kompetencija imaju učitelji i nastavnici, zbog čega preporučuju revidiranje programa temeljnog profesionalnog obrazovanja učitelja na fakultetima, te evaluaciju postojećih programa informatike u školama. Razlog ovome vide u nedostatku didaktičkih materijala u školama, tj. nedostatnoj opremljenosti škola te nepostojanju cjeloživotnih programa obrazovanja učitelja i nastavnika na temu *cyber* sigurnosti djece i mladih. Posljednje smatraju posebno problematičnim jer su zabilježili porast *online* programa osposobljavanja i usavršavanja (webinara) kojima je tema *cyber* nasilje i rizici korištenja interneta kod djece, dok izostaju programi cjeloživotnoga obrazovanja učitelja i nastavnika za njih same tj. odrasle kao korisnike interneta. Upravo jačanje temeljnih kompetencija učitelja i nastavnika za samostalno i što sigurnije korištenje interneta treba biti osnova na kojoj će se graditi sigurnost djece i mladih.

3.3.1.2. Spolne razlike u znanju i rizičnom ponašanju računalnih korisnika

Istraživanjem se također htjelo provjeriti razlikuju li se muškarci od žena u rizičnom *online* ponašanju te u svojem znanju o informacijskoj sigurnosti. Kako je dobiven značajni glavni učinak spola (MANOVA, Tablica 5.) Hochbergovim post-hocom testom utvrđene su spolne razlike za svaku skalu i subskalu UZPK-a.

Tablica 7. Prikaz spolnih razlika za pojedine skale i subskale UZPK-a

UZPK	Spol	M	SD	$F_{(1,4858)}$
Skala rizičnog ponašanja računalnih korisnika	muško	3,98	0,45	0,04
	žensko	4,01	0,39	
Skala znanja o informacijskog sigurnosti	muško	2,99	0,56	8,67**
	žensko	3,12	0,50	
Subskala posuđivanja pristupnih podataka	muško	4,67	0,55	2,09
	žensko	4,67	0,45	
Subskala održavanja osobnih računalnih sustava	muško	3,26	0,90	1,47
	žensko	3,28	0,78	
Subskala uobičajenih rizičnih ponašanja korisnika računala	muško	4,13	0,66	3,02
	žensko	4,18	0,55	

Subskala stupnja sigurnosti računalne komunikacije	muško	2,92	0,90	0,00
	žensko	2,93	0,76	
Subskala uvjerenja o sigurnosti računalnih podataka	muško	2,22	0,91	3,21
	žensko	2,38	0,85	
Subskala važnosti pravilne pohrane računalnih podataka	muško	3,70	0,86	8,88**
	žensko	3,90	0,72	

*p < 0,05; **p < 0,01

Spolne razlike dobivene su samo za skalu znanja, odnosno subskalu važnosti pravilne pohrane računalnih podataka, pri čemu su ženske sudionice pokazale veće znanje od muških sudionika. Prijašnja su istraživanja jasno pokazala kako su žene su u odnosu na muškarce opreznije i skeptičnije u otkrivanju privatnih podataka (Šolić, Velki i Galba, 2015; Velki i sur., 2017).

U svojemu istraživanju, ENISA (2014) ne pronalazi statistički značajne razlike u korištenju interneta i rizičnim ponašanjima muškaraca i žena. Ipak, važno je reći kako njihovo istraživanje bilo o učestalosti korištenja interneta, bez naznačavanja o kojoj komponenti se radi (znanje, iskustvo ili nešto treće). Stoga se može zaključiti kako su potrebna dodatna istraživanja u odnosu na različite varijable kao što su osobine ličnosti ili kulturološka praksa korištenja interneta, te svakako socijalni konformizam koji pritom sudionici istraživanja mogu iskazati.

Istražujući korištenje interneta u odnosu na spol sudionika istraživanja, Helsper (2010) zaključuje kako su razlike u spolu manje u razvijenijim društvima u kojima dječaci i djevojčice imaju podjednake prilike za stjecanje informatičkih kompetencija, u kojima je i dječacima i djevojčicama internet jednako dostupan i u društvima u kojima se informatičko opismenjavanja dječaka i djevojčica izvodi u jednakim odgojno-obrazovnim uvjetima. Ukoliko se uzmu u obzir njezina tumačenja, moglo bi se zaključiti kako je Republika Hrvatska još uvijek u procesu tranzicije društva iz tradicionalističkog u suvremeno.

3.3.1.3. Razlike u znanju i rizičnom ponašanju računalnih korisnika u odnosu na odavanje zaporke

Prijašnja istraživanja su jasno pokazala kako velik broj osoba odaje svoju zaporku (Velki, Šolić i Nenadić, 2015). Željelo se provjeriti razlikuju li se osobe koje odaju svoju zaporku u odnosu na osobe koje ne odaju svoju zaporku u rizičnom *online* ponašanju te u svojem znanju o informacijskoj sigurnosti. Kako je dobiven značajni glavni učinak odavanja zaporke (MANOVA, Tablica 5.) Hochbergovim post-hocom testom utvrđene razlike u odavanju zaporke za svaku skalu i subskalu UZPK-a.

Tablica 8. Prikaz razlika u odavanju zaporke za pojedine skale i subskale UZPK-a

UZPK	Odavanje zaporke	M	SD	$F_{(1,4661)}$
Skala rizičnog ponašanja računalnih korisnika	da	3,99	0,42	13,37**
	ne	4,00	0,42	
Skala znanja o informacijskoj sigurnosti	da	3,08	0,52	1,77
	ne	3,04	0,54	
Subskala posuđivanja pristupnih podataka	da	4,67	0,49	2,42
	ne	4,66	0,49	
Subskala održavanja osobnih računalnih sustava	da	3,27	0,84	26,18**
	ne	3,31	0,81	
Subskala uobičajenih rizičnih ponašanja korisnika računala	da	4,15	0,59	1,36
	ne	4,16	0,60	
Subskala stupnja sigurnosti računalne komunikacije	da	2,92	0,80	0,76
	ne	2,91	0,83	
Subskala uvjerenja o sigurnosti računalnih podataka	da	2,34	0,88	1,381
	ne	2,29	0,87	
Subskala važnosti pravilne pohrane računalnih podataka	da	3,83	0,79	0,23
	ne	3,80	0,78	

*p < 0,05; **p < 0,01

Za sudionike koji odaju svoju zaporku, u odnosu na one koji ju ne odaju, dobivena je statistički značajna razlika na skali rizičnog ponašanja računalnih korisnika, odnosno na subskali održavanja računalnih sustava, i to u neočekivanom smjeru. Osobe koje ne odaju zaporku pokazuju statistički značajno više rizičnog ponašanja, odnosno lošije održavaju osobne računalne sustave, što je u suprotnosti s prijašnjim istraživanjima (Šolić, Velki i Galba, 2015). Očito stvarno ponašanje odavanja zaporke ne igra značajnu ulogu u znanju o informacijskim sustavima, a niti u rizičnom ponašanju vezanom uz korištenje informacijskih sustava, već je odraz ponašajnog stila osoba. Odnosno, kako kaže Starčević (2015), korištenje interneta i stilova ponašanja u značajnoj je mjeri određeno osobinama ličnosti. Treba napomenuti da istraživači nisu bili u mogućnosti provjeriti jesu li sudionici zaista dali svoju aktivnu zaporku pa je moguće da su neočekivani rezultati dobiveni zbog davanja neiskrenih odgovora sudionika (odnosno odavanja lažne zaporke).

3.3.1.4. Interakcijski učinci MANOVA

Interakcijski učinak predstavlja učinak istovremenog uzajamnog djelovanja dvaju čimbenika (npr. spol i dob) na način da se utjecaj jednog čimbenika na neku

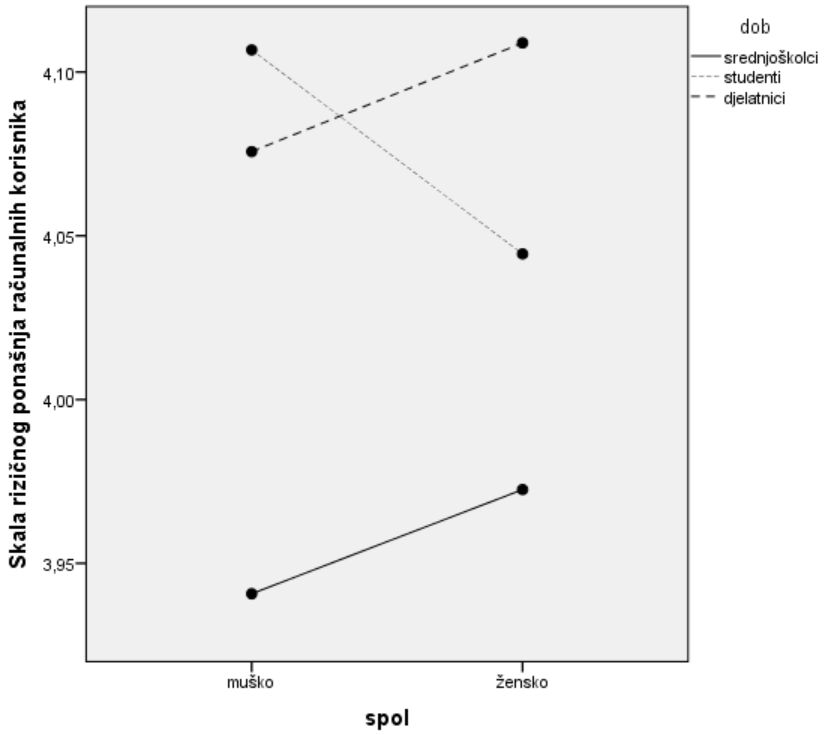
zavisnu varijablu (npr. rizično *online* ponašanje) mijenja ovisno o razini drugog čimbenika. Npr. dob, znači ni srednjoškolci, ni studenti ni odrasli zaposlenici, nemaju utjecaja na rizično *online* ponašanje kod muških sudionika, ali imaju utjecaja na žene, i to tako da žene što su starije pokazuju manje rizičnog *online* ponašanja.

Tablica 9. Prikaz interakcijskih učinaka za pojedine skale i subskale UZPK-a

interakcija	UZPK	F
dob x spol	Skala rizičnog ponašanja računalnih korisnika	3,37*
	Subskala posuđivanja pristupnih podataka	1,63
	Subskala održavanja osobnih računalnih sustava	4,17*
	Subskala uobičajenih rizičnih ponašanja korisnika računala	0,55
	Skala znanja o informacijskoj sigurnosti	9,92**
	Subskala stupnja sigurnosti računalne komunikacije	1,53
	Subskala uvjerenja o sigurnosti računalnih podataka	9,97**
	Subskala važnosti pravilne pohrane računalnih podataka	6,74**
dob x zaporka	Skala rizičnog ponašanja računalnih korisnika	1,96
	Subskala posuđivanja pristupnih podataka	1,27
	Subskala održavanja osobnih računalnih sustava	2,20
	Subskala uobičajenih rizičnih ponašanja korisnika računala	0,81
	Skala znanja o informacijskog sigurnosti	0,72
	Subskala stupnja sigurnosti računalne komunikacije	2,15
	Subskala uvjerenja o sigurnosti računalnih podataka	1,24
	Subskala važnosti pravilne pohrane računalnih podataka	3,14*
spol x zaporka	Skala rizičnog ponašanja računalnih korisnika	0,01
	Subskala posuđivanja pristupnih podataka	2,93
	Subskala održavanja osobnih računalnih sustava	2,45
	Subskala uobičajenih rizičnih ponašanja korisnika računala	3,03*
	Skala znanja o informacijskoj sigurnosti	1,41
	Subskala stupnja sigurnosti računalne komunikacije	0,54
	Subskala uvjerenja o sigurnosti računalnih podataka	0,63
	Subskala važnosti pravilne pohrane računalnih podataka	2,91
dob x spol x zaporka	Skala rizičnog ponašanja računalnih korisnika	1,23
	Subskala posuđivanja pristupnih podataka	2,18
	Subskala održavanja osobnih računalnih sustava	2,40
	Subskala uobičajenih rizičnih ponašanja korisnika računala	5,49**
	Skala znanja o informacijskog sigurnosti	2,24
	Subskala stupnja sigurnosti računalne komunikacije	0,32
	Subskala uvjerenja o sigurnosti računalnih podataka	2,09
	Subskala važnosti pravilne pohrane računalnih podataka	4,12*

*p < 0,05; **p < 0,01

U Tablici 9. prikazani su rezultati interakcijskih učinaka. Najviše značajnih učinaka dobiveno je za interakciju dob x spol. Radi lakše interpretacije svi značajni učinci prikazani su na grafovima (od X do Y).

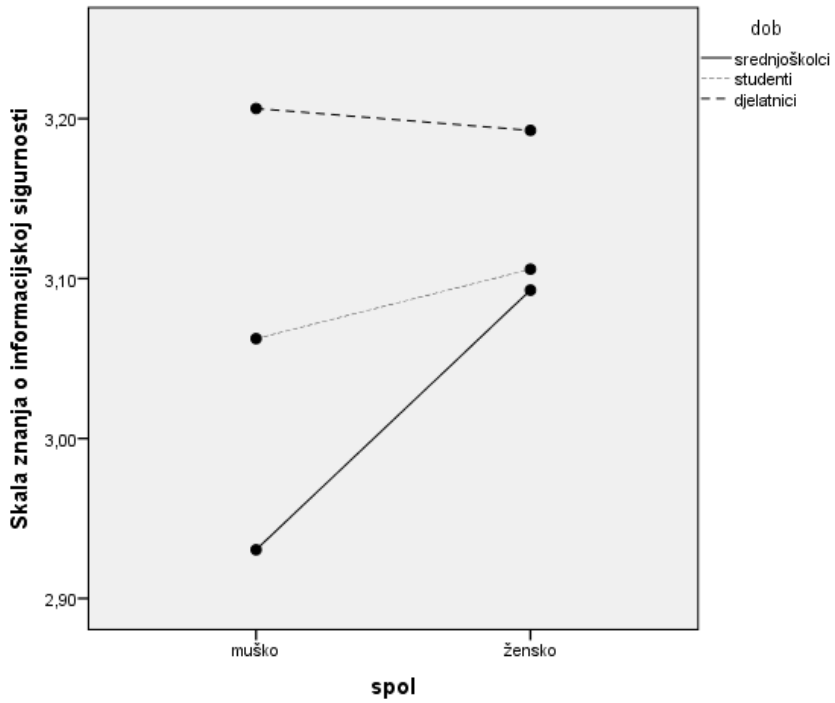


Slika 3.
Prikaz interakcijskog učinka spol x dob za skalu rizičnog ponašanja računalnih korisnika

Na Slici 3. prikazan je interakcijski učinak dob x spol za skalu rizičnog ponašanja računalnih korisnika. Mlađi i stariji muškarci (srednjoškolci i odrasli zaposlenici) pokazuju manje rizičnog ponašanja u odnosu na muške studenti dok kod žena s porastom dobi dolazi do smanjenja rizičnog *online* ponašanja. Kod mlađih i starijih skupina sudionika oprezniji je muški spol, dok u skupini srednje dobi više opreza pokazuju studentice što je očekivano jer su žene i u prijašnjim istraživanjem pokazivale opreznije ponašanje (Šolić, Velki i Galba, 2015; Velki i sur., 2017).

Istražujući navike korisnika interneta po spolu, Helsper (2010) pronalazi kako za istraživanje korištenja interneta po spolu ključna kronološka dob ispitanika. Naime, odrasli različite kronološke dobi imaju različite uloge, ovisno o tome jesu

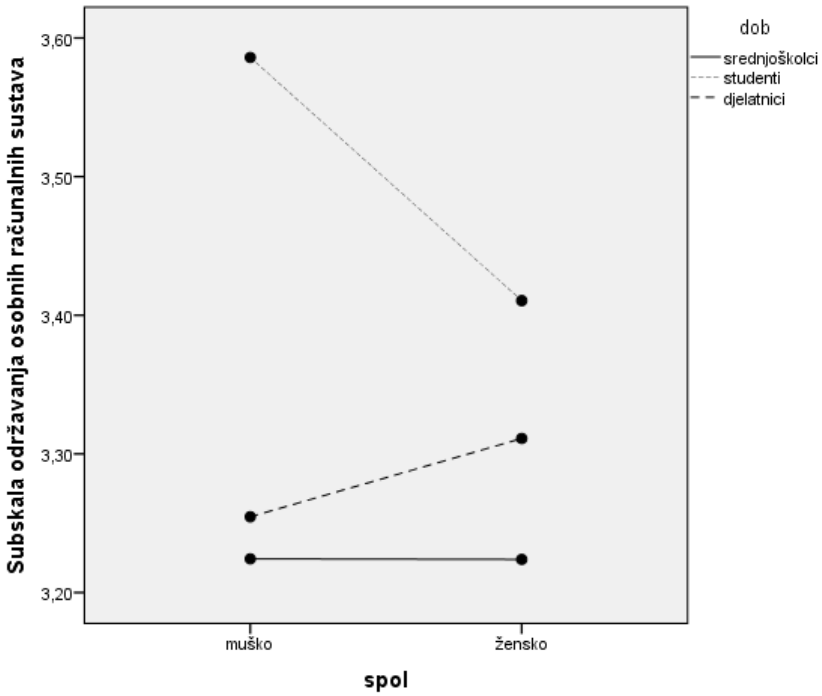
li samci ili u vezi/braku, imaju li djecu ili ne, koje su kronološke dobi njihova djeca itd., pa to određuje što će korisnici pretraživati i na koji način. Odnosno, manje je bitno kojega su spola, već se bilježi postojanje međusobne povezanosti spola i kronološke dobi. U tom kontekstu, neočekivani rezultati za mlađe i starije skupine sudionika (srednjoškolci i djelatnici) u vidu manje rizičnog ponašanja muškog spola ovdje se mogu interpretirati i zbog svrhe korištenja računalnih sustava upravo u odnosu na kronološku dob, pri čemu ih mladići više koriste za igranje računalnih igrica, a muškarci za posao, dok ih djevojke više koriste za komunikaciju i *online* kupnju.



Slika 4.
Prikaz interakcijskog učinka spol x dob za skalu znanju o informacijskoj sigurnosti

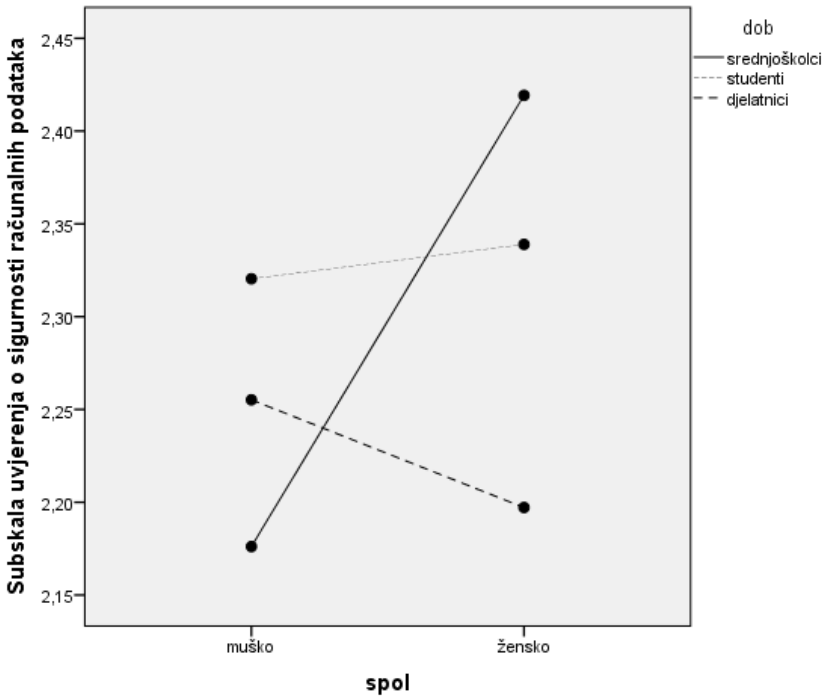
Na Slici 4. prikazan je interakcijski učinak dob x spol za skalu o informacijskoj sigurnosti. Srednjoškolci i studenti, posebice muškarci pokazuju manje znanja o informacijskoj sigurnosti. Mlađi muškarci (srednjoškolci i studenti) pokazuju najmanje znanja (u odnosu na mlađe žene), dok je u starijoj dobi suprotna situacija gdje je općenito najviša razina znanja, ali u ovom slučaju žene pokazuju čak višu razinu znanja. Porastom dobi dolazi i do porasta znanja o informacijskoj

sigurnosti, ali se odnos znanja mijenja ovisno o spolu osoba, gdje u mlađoj dobi ženski sudionici pokazuju više znanja o informacijskoj sigurnosti, a u starijoj dobi to su muški sudionici. Moguće je da djelatnici, muškarci, češće rade na mjestima u kojima se više zahtijeva korištenje računalnih sustava, pa su stoga i obrazovaniji i upoznatiji s činjenicama vezanim uz informacijsku sigurnost, dok u mlađoj dobi više znanja pokazuje ženski spol (posebice srednjoškolke) što može biti i odraz formalnog obrazovanja, u kojemu su češće djevojke bolje učenice od mladića, pa je stoga moguće i da posjeduju bolja znanja o informacijskoj sigurnosti. Uzimajući u obzir neka prethodna istraživanja korištenja interneta i rizičnih ponašanja po spolu (Helsper, 2010; ENISA, 2014) u kojima se raspravljalo i o kulturološkim čimbenicima tj. utjecajima društvene prakse odgoja i obrazovanja dječaka i djevojčica na kasnije ponašanje na internetu, može se zaključiti kako nedostaje dovoljno pouzdanih informacija o izvanjskim čimbenicima koji mogu utjecati na ponašanja korisnika te bi ih bilo poželjno istraživati dodatnim subskalama ili uvođenjem kvalitativne metodologije u istraživanja na ovom području.



Slika 5.
Prikaz interakcijskog učinka spol x dob za subskalu održavanja osobnih računalnih sustava

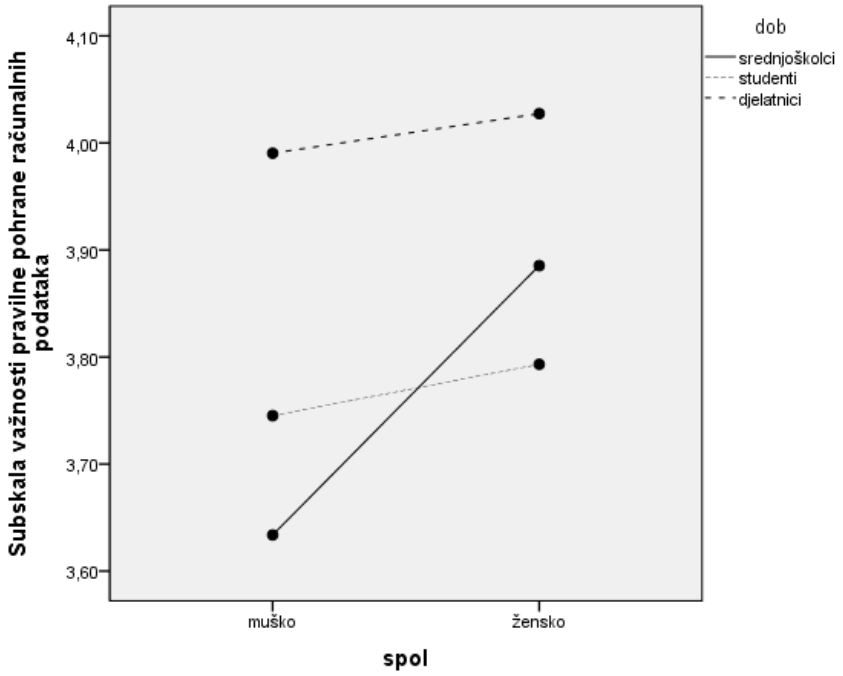
Na Slici 5. prikazan je interakcijski učinak dob x spol za subskalu održavanja osobnih računalnih sustava. Dok za srednjoškolce ne uočavamo razliku u spolu, za starije sudionike (djelatnici) uočavamo da ženski sudionici slabije održavaju osobna računala što je u suprotnosti sa studentima među kojima muški spol slabije održava računala. Pretpostavka je da je još uvijek više muških djelatnika radi u sektorima koji se bave održavanjem informacijskih sustava, stoga porastom životne dobi, održavanje računalnih sustava postaje važnije za muške u odnosu na ženske sudionike.



Slika 6.
Prikaz interakcijskog učinka spol x dob za subskalu uvjerenja o sigurnosti računalnih podataka

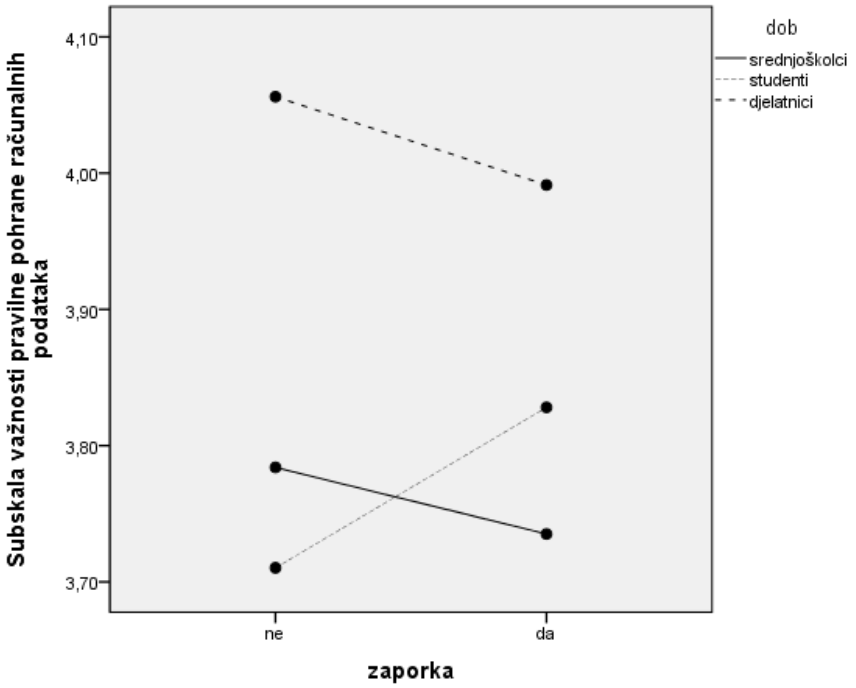
Na Slici 6. prikazan je interakcijski učinak dob x spol za subskalu uvjerenja o sigurnosti računalnih podataka. Dok za mlađe sudionike (srednjoškolce i studente) uočavamo isti trend, pri čemu višu razinu znanja o sigurnosti računalnih podataka pokazuju ženske sudionice (posebice srednjoškolke), suprotno je dobiveno za starije sudionike (djelatnike) kod kojih muškarci pokazuju viša znanja o sigurnosti računalnih podataka. Za mlađe sudionike bolje znanje ženskog spola može biti odraz formalnog školovanja, kod starijih sudionika bolje znanje

muškog spola može biti odraz zaduženja na radnom mjestu, odnosno općenito poslova koje obavljaju.



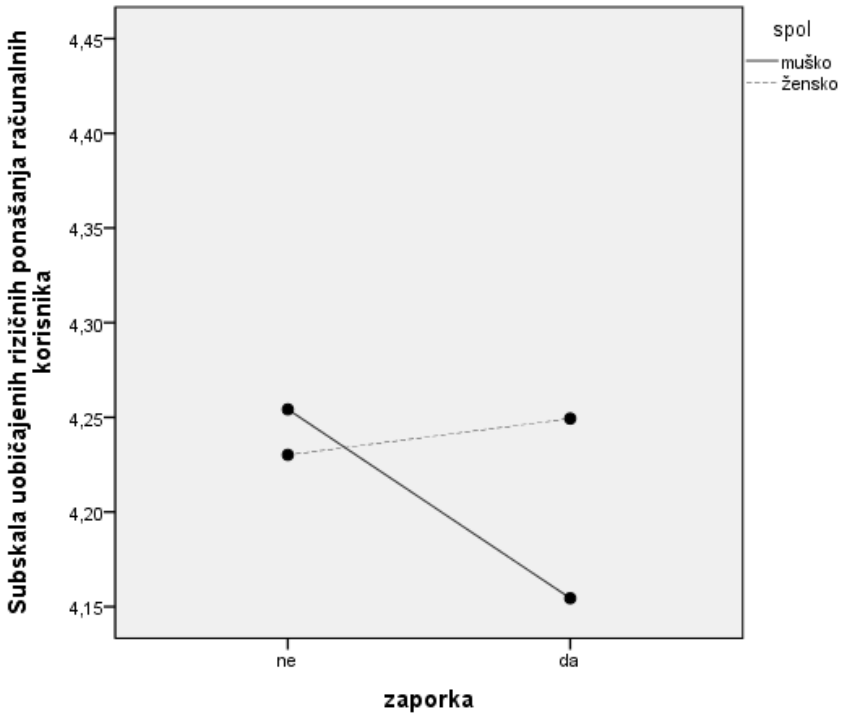
Slika 7.
Prikaz interakcijskog učinka spol x dob za subskalu važnosti pravilne pohrane računalnih podataka

Na Slici 7. prikazan je interakcijski učinak (međusobni odnos) varijabli dobi i spola u odnosu na važnost pravilne pohrane računalnih podataka. Dok za studente i zaposlenike uočavamo isti trend blagog povećanja znanja o važnosti pravilne pohrane s porastom dobi, posebice za ženske sudionice, kod srednjoškolaca se, za muški spol, jasno vidi najniža razina znanja o važnosti pravilne pohrane, dok je nagli porast dobiven za ženski spol, te je kod srednjoškolki viša razina znanja u odnosu na muški spol, ali i u odnosu na oba spola studentske populacije. Svjesnost o važnosti pravilne pohrane podataka, odnosno mogući rizici pri gubitku računalnih podataka, viša je kod ženskog spola, što je sukladno prijašnjim istraživanjima koja pokazuju veću opreznost žena (Šolić, Velki i Galba, 2015; Velki i sur., 2017).



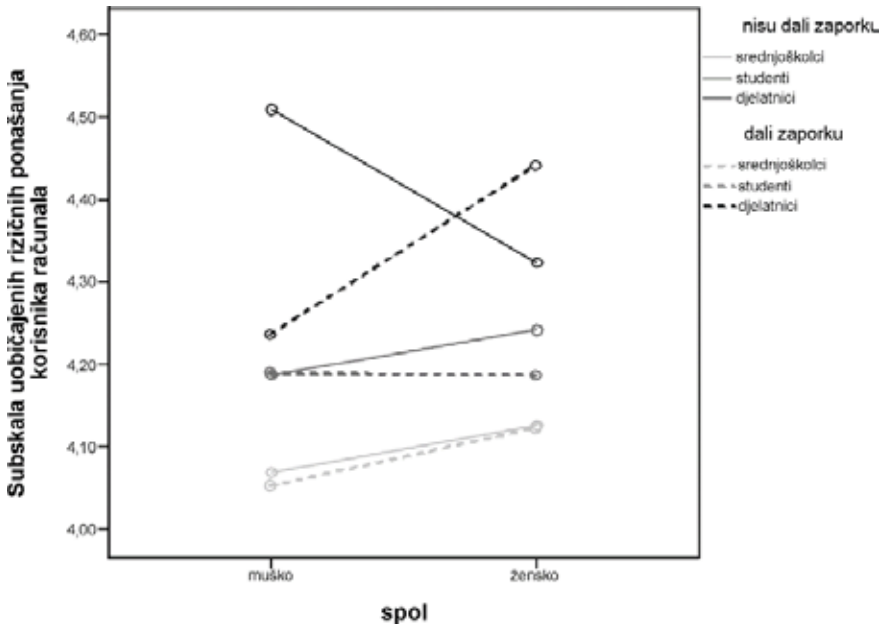
Slika 8.
Prikaz interakcijskog učinka zaporka x dob za subskalu važnosti pravilne pohrane računalnih podataka

Na Slici 8. prikazan je interakcijski učinak dob x zaporka za subskalu važnosti pravilne pohrane računalnih podataka. Dok za srednjoškolce i zaposlenike uočavamo isti trend gdje osobe koje ne odaju svoju zaporku pokazuju i višu razinu znanja vezanu uz pravilnu pohranu računalnih podataka, za studente je dobiven suprotan trend. Studenti koji odaju svoj zaporku imaju i više znanja o važnosti pravilne pohrane računalnih podataka, što opet ide u prilog činjenici da samo znanje nije zaštitni čimbenik za rizična ponašanja računalnih korisnika, odnosno kao što su i prijašnja istraživanja pokazala osobe koje imaju veću razinu znanja sklonije su rizičnije se ponašati (Velki i sur., 2017). Međutim treba uzeti u obzir da zbog zaštite privatnosti podataka istraživači nisu bili u mogućnosti provjeriti valjanost odanih zaporki, odnosno jesu li sudionici istraživanja dali valjanu aktivnu zaporku ili lažnu.



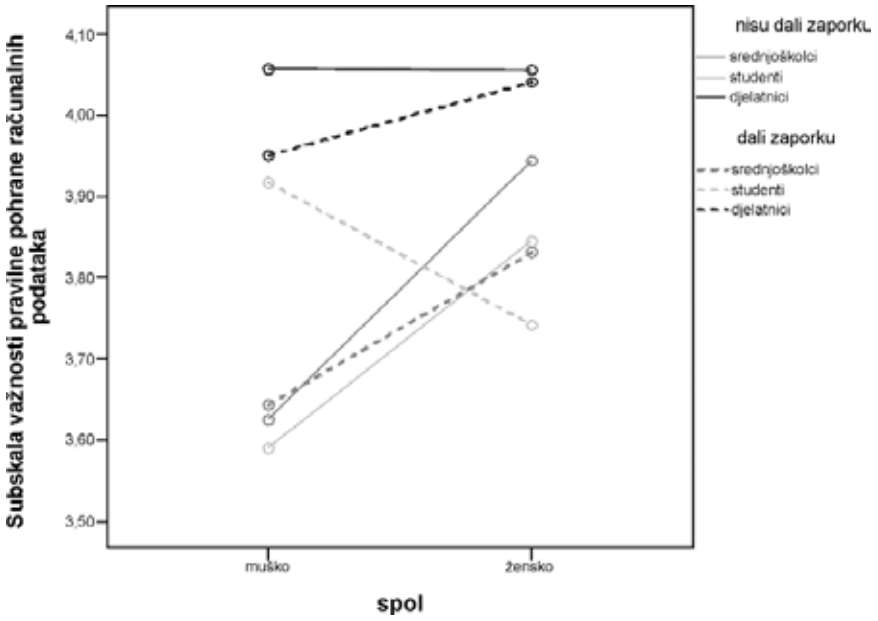
Slika 9.
Prikaz interakcijskog učinka zaporka x spol za subskalu uobičajenih rizičnih ponašanja računalnih korisnika

Na Slici 9. prikazan je interakcijski učinakspol x zaporka za subskalu uobičajenih rizičnih ponašanja računalnih korisnika. Muške osobe koje češće odaju zaporku pokazuju manje ostalih rizičnih ponašanja dok ženske osobe koje odaju zaporku pokazuju više rizičnih ponašanja računalnih korisnika što je očekivano jer samo odavanje zaporke predstavlja oblik rizičnog *online* ponašanja. Dok je ponašanje ženskih sudionica u skladu s očekivanjima, ponašanje muških sudionika je u suprotnosti, odnosno moguće je da stvarno ponašanje tj. odavanje zaporke kod muškarca ne predstavlja dobro ostala rizična *online* ponašanja za koja oni procjenjuju da čine. Moguće je i da muške izjave nisu u skladu s njihovim stvarnim ponašanjem, dok je kod ženskih sudionica uočena veća konzistentnost ponašanja i mišljenja. O prisutnosti socijalnog konformizma u istraživanjima rizičnih ponašanja u postojećoj literaturi se uopće ne govori, no dobiveni podatci ukazuju kako bi se u budućim istraživanjima moglo dodatnim subskalama provjeriti postojanje ove varijable koja može utjecati na statističku obradu i kasnije interpretaciju prikupljenih i obrađenih podataka.



Slika 10.
Prikaz interakcijskog učinka zaporka x spol x dob za subskalu uobičajenih rizičnih ponašanja računalnih korisnika

Na Slici 10. prikazan je interakcijski učinak spol x dob x zaporka za subskalu važnosti pravilne pohrane računalnih podataka. Odavanje zaporke za srednjoškolce ne igra ulogu te ostaje isti trend u kojem srednjoškolci muškog spola imaju manje znanja vezano uz pravilnu pohranu računalnih podataka za razliku od srednjoškolki. Starije dobne skupine pokazuju drugačiji trend. Studenti muškog spola pokazuju jednako uobičajenih rizičnih ponašanja neovisno o tome jesu li dali zaporku, dok studentice koje su dale zaporku pokazuju manje rizičnih ponašanja. Za djelatnike su dobivene veće razlike. Muški djelatnici koji nisu dali zaporku pokazuju najviše rizičnih ponašanja, dok ženske djelatnice koje su dale zaporku pokazuju najviše rizičnog ponašanja računalnih korisnika. Stariji sudionici, muškog spola koji nisu dali zaporku pokazuju više rizičnih ponašanja pri čemu je očito da samo odavanje zaporke nije ključno za ostala rizična ponašanja korisnika računala već varijable dobi i posla kod ove skupine tome više pridonose. Starije sudionice ženskog spola ukoliko su dale zaporku pokazuju više rizičnog ponašanja što je u skladu s konzistentnošću njihova ponašanja i mišljenja, dok mlađe sudionice ženskog spola koje nisu dale zaporku pokazuju više uobičajenog rizičnog ponašanja računalnih korisnika, odnosno manja je konzistentnost ponašanja i mišljenja, što je i očekivano za srednjoškolsku populaciju.



Slika 11.
Prikaz interakcijskog učinka zaporka x spol x dob za subskalu važnosti pravilne pohrane računalnih podataka

Na Slici 11. prikazan je interakcijski učinak spol x dob x zaporka za subskalu važnosti pravilne pohrane računalnih podataka. Za sve sudionice (ženski spol) višu razinu znanja o važnosti pravilne pohrane podataka pokazuju sudionice koje nisu dale svoje zaporku, što je u skladu i s prijašnjim istraživanjima o većoj savjesnosti i opreznosti kod žena (Šolić, Velki i Galba, 2015). Međutim za muški spol dobivene su drugačiji rezultati. Za mlađe muške sudionike (srednjoškolci i studenti) višu razinu znanja o pravilnoj pohrani podataka pokazuju oni koji su dali svoju zaporku što je u skladu s prijašnjim istraživanjima gdje osobe koje posjeduju određena znanja su sklonije rizičnijem ponašanju kao što je odavanje zaporke (Velki i sur., 2017), dok stariji sudionici (djelatnici) pokazuju višu razinu znanja o važnosti pravilne pohrane računalnih podataka ukoliko nisu dali svoju zaporku, što je u skladu s konzistentnošću ponašanja i mišljenja, posebice za stariju dob.

3.3.1.5. Odnos između znanja o informacijskoj sigurnosti i rizičnog ponašanja računalnih korisnika

Naposljetku smo htjeli ispitati odnos između znanja o informacijskoj sigurnosti i rizičnog ponašanja računalnih korisnika. Neka prijašnja istraživanja go-

vore u prilog tome da što osoba posjeduje veće znanje o informacijskoj sigurnosti, sklonije je rizičnije se ponašati (Šolić i Ilakovovac, 2009; Šolić, i sur., 2009; Velki i sur., 2017).

Tablica 10. Povezanost skala i subskala UZPK-a (svi sudinici, N=4859)

	SRP	SZS	PP	OS	RP	SS	US	VS
Skala rizičnog ponašanja računalnih korisnika - SRP	-	,200**	,585**	,691**	,624**	,050**	-,048**	,369**
Skala znanja o informacijskog sigurnosti - SZS		-	,075**	,207**	,058**	,567**	,675**	,660**
Subskala posuđivanja pristupnih podataka - PP			-	,034*	,429**	,032*	-,080**	,181**
Subskala održavanja osobnih računalnih sustava - OS				-	-,039**	-,031*	,057**	,353**
Subskala uobičajenih rizičnih ponašanja korisnika računala - RP					-	,120**	-,120**	,117**
Subskala stupnja sigurnosti računalne komunikacije - SS						-	,118**	,028
Subskala uvjerenja o sigurnosti računalnih podataka - US							-	,174**
Subskala važnosti pravilne pohrane računalnih podataka - VS								-

** p < 0,01; * p< 0,05

U Tablici 10. su prikazani rezultati korelacijske analize za sve skale i subskale UZPK-a. Skala rizičnog ponašanja računalnih korisnika i Skala znanja o informacijskoj sigurnosti su u maloj, ali statistički značajnoj povezanosti što znači da osobe koje posjeduju višu razina znanja ujedno čine i više rizičnih ponašanja. Općenito je isti trend dobiven i za većinu subskala. Za subskalu uobičajenih rizičnih ponašanja dobivena je vrlo mala statistički značajna negativna povezanost sa subskalom održavanja računalnih sustava i sa subskalom stupnja sigurnosti računalne komunikacije, što bi značilo da osobe koje bolje održavaju računalne sustave ujedno pokazuju i više rizičnih *online* ponašanja, te manje znanja vezanih uz sigurnu računalnu komunikaciju. Subskala uvjerenja o sigurnosti računalnih podataka pokazala je malu statistički značajnu negativnu povezanost sa skalom rizičnog ponašanja računalnih korisnika te subskalama posuđivanja pristupnih podataka i uobičajenih rizičnih ponašanja. Osobe koje posjeduju veća znanja i uvjerenja o sigurnosti računalnih podataka ujedno pokazuju manje rizičnih

ponašanja, odnosno rjeđe posuđuju vlastite pristupne podatke drugim osobama te općenito iskazuju nižu razinu uobičajenih rizičnih ponašanja računalnih korisnika. Iako u nekim slučajevima znanje, odnosno svjesnost o informacijskoj sigurnosti, može biti zaštitni čimbenik za *online* rizična ponašanja, ipak se u većini slučajeva viša razina znanja pokazala kao rizik za dodatna problematična *online* ponašanja. Ovaj trend je u skladu s rezultatima prijašnjih studija koje su pokazale na različitim dobnim uzorcima kako osobe koje posjeduju viša znanja i svjesnije su potencijalne opasnosti ujedno se i rizičnije ponašaju pri korištenju informacijskih sustava (Šolić i Ilakovovac, 2009; Šolić, i sur., 2009; Velki i sur., 2017). Samo znanje i svijest o tome da osoba nešto zna, stvara lažni osjećaj sigurnosti u računalnih korisnika te pridonosi tome da ne paze i ne pridržavaju se naučenih pravila vezanih uz informacijsku sigurnost.

3.4. ZAKLJUČAK

Provedenim istraživanjem je utvrđen obrazac ponašanja različitih sudionika o informacijskoj sigurnosti. Zaposlenici pokazuju najviši stupanj znanja, ali i rizičnog ponašanja, iza njih odmah slijede studenti, dok srednjoškolci posjeduju najmanje znanja vezanih uz informacijsku sigurnost, ali i najmanje rizičnih ponašanja korisnika računalnih sustava. Dobivena je i pozitivna povezanost između skala znanja i skala rizičnog ponašanja, odnosno što pojedinci pokazuju viši stupanj znanja o informacijskoj sigurnosti, ujedno pokazuju i viši stupanj rizičnog ponašanja računalnih korisnika. Ovo ide u prilog činjenici da visoko znanje ne predstavlja zaštitu od rizičnog *online* ponašanja, odnosno da su u prevenciji *online* rizika potrebe dodatne mjere, a ne samo osviještenost sudionika i njihova razina znanja.

Spolnih razlika, kao i razliku u odavanju zaporke na pojedinim skalama i subskalama gotovo nije bilo, što ide u prilog univerzalnosti primjene UZPK-a. Upitnik se može primjenjivati na različitim uzorcima što mu je glavna snaga i prednost.

Dobiveni rezultati su u značajnoj mjeri slični onima koji su dobiveni u istraživanjima unutar zemalja EU-a (ENISA, 2014), u kojima RH nije prethodno sudjelovala. Praktične implikacije koje se pritom nameću mogu se podijeliti u tri velike skupine: (1) kulturni kontekst – stilovi odgoja u pojedinim kulturama, (2) zakonski okviri – zakonska regulacija uporabe interneta i (3) odgojno-obrazovni kontekst – opremljenost škola i prisutnost programa informatike. Zakonska se ograničenja za RH odnose na sprječavanje distribucije neprimjerenih sadržaja i sadržaja koji podliježu autorskim pravima, no posebnih zakonskih ograničenja

nema, te su česte internetske prijevare putem e-pošte u obliku dobitaka, nasljeđivanja i sl. što pružatelji internetskih usluga ne filtriraju u dovoljnoj mjeri. Kulturni kontekst se odnosi na stilove odgoja i viđenje djeteta u pojedinim kulturama. Tako se u zapadnim i skandinavskim kulturama djeca vide kao aktivni građani koji participiraju u svojemu društvu te djeca i mladi u navedenom području u većem postotku koriste internet bez nadzora roditelja. Također, u tim zemljama su češće prisutni tzv. *child-friendly* alati kojima djeca mogu nesmetano pretraživati internet, bez straha roditelja da će tijekom surfanja naići na neprimjerene sadržaje. S druge strane, u državama koje su tradicionalno orijentirane (južna i istočna Europa), građani općenito u manjem postotku koriste internet, njihova djeca su manje *online*, ali kada jesu nemaju mogućnost softverske zaštite od nepoželjnih sadržaja. Kulturni kontekst uvelike određuje stilove ponašanja korisnika svih kronoloških dobi, što bi i u budućnosti bilo zanimljivo propitati. Naposljetku – ključ je odgojno-obrazovni kontekst, što se može naslutiti i iz dobivenih rezultata ovdje. Prisutnost primjerenih i suvremenih programa informatike je početna stepenica u podizanju informacijske pismenosti djece i mladih. Uvidom u udžbenike informatike, vidljivo je kako su prve lekcije uglavnom usmjerene na dijelove računala, uključujući diskete, iako istraživanje Livingstonea i Haddona (2009) pokazuje kako djeca počinju koristiti internet vrlo rano, čak u prve tri godine života. To znači kada se počnu obrazovati u sklopu informatike u osnovnim školama veliki broj djece već ima višegodišnje iskustvo korištenja interneta. U prilog potrebi kvalitetnijih programa informatike, već od najranije dobi, govori i statistika korištenja interneta na razini EU-a: 60% djece u dobi od 6 do 10 godina koristi internet te taj postotak raste sve do 86% za dob od 15 do 17 godina. Prosječno 75% djece i mladih u dobi od 7 do 18 godina koriste internet, dok je odraslih korisnika još više (84%).

3.5. PREPORUKE

Stoga bi se preporuke za rad na temelju provedenoga istraživanja mogle razvrstati u odnosu na rizike koji su ovdje zabilježeni, a to su u prvome redu zaštita osobnih podataka i praćenje protokola sigurnosti. U tom dijelu moguće je činiti sljedeće:

- ukloniti osobne podatke s profila ili korisničkih računa (ime, prezime, adresa, detalji o školovanju, fotografije i zaporke),
- kod kreiranja zaporke kombinirati velika i mala slova i brojeve,
- za različite korisničke račune osmisliti različita imena i zaporke,
- osigurati pristup korisničkom računu sigurnosnim pitanjem,

- instalirati programe zaštite računala i redovito održavati sustav,
- održavati računalo – brisati nepotrebne dokumente i sadržaje što će rasteretiti memoriju računala i omogućiti bolji rad,
- koristiti nadimak/alias u komunikaciji, koristiti avatare,
- u slučaju neprimjerene komunikacije, blokirati osobu ili ju prijaviti administratoru,
- kod pretraživanja sadržaja koristiti napredne postavke ili ključne riječi kojima će se suziti izbor sadržaja i otvaranja linkova,
- instalirati dodatne programe koji omogućuju zaštitu ili blokiranje neprimjerenih sadržaja,
- provjeravati sigurnost mrežnih stranica i profile administratora,
- kod *online* kupovine koristiti se provjerenim stranicama i/ili karticom koja ima samo onaj iznos koji je potreban za kupovinu (neka to ne budu kartice tekućih računa ili kartica na kojima imate ušteđevinu),
- informirati se o potencijalnim prijetnjama u odnosu na mrežne stranice koje posjećujete,
- prihvaćanje poruka i *online* prijateljstava samo od poznatih osoba tj. osoba koje poznajete i u stvarnom životu,
- provjeriti štetnost sadržaja koje primate s molbom za prosljeđivanjem drugim korisnicima,
- poštovati pravila komunikacije na portalima, *online* grupama i drugim oblicima virtualnog okupljanja (*chat rooms*, blogovi, forumi i sl.) itd.

Navedene preporuke su temeljni preduvjeti sigurnosti, no stalni oprez i kontrola podataka su potrebni kako bi se održala primjerena razina sigurnosti i reducirali *online* rizici.

3.6. LITERATURA

Crossler, R. E., Johnston, A. C., Lowry, P. B, Hu, Q., Warkentin, M. i Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32,* 90-101.

Dell'Amico, M., Michiardi, P. i Roudier, Y. (2010). Password Strength: An Empirical Analysis. *Proceedings IEEE INFOCOM,* 1-9.

ENISA (2014). *Roadmap for NS education programmes in Europe.* Madrid: ENISA.

Haley, K. (2011). *Information robbery - The 2011 Internet security threat report. InfoSecToday*. Preuzeto s http://www.infosectoday.com/Articles/Information_ Robbery.htm, 3. 5. 2018.

Helsper, E. (2010). Gendered internet use across generations and life stages. *Communication Research, 37,* 352-374.

Kelley, P. G. i sur. (2012). Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms. *IEEE Symposium on Security and Privacy,* 523-537.

Kwang, K. i Choo, R. (2011). The cyberthreat landscape: Challenges and future research directions. *Compures & Security, 30,* 719-731.

Livingstone, S. i Haddon, L. (2009). *EU Kids online: Final report.* London: EC safer Internet/EU Kids online.

Lukasik, S. J. (2011). Protecting Users of the Cyber Common. *Communications of the ACM, 54*, 54-61.

Mitnick, K. D., Simon, W. L. i Wozniak S. (2002). *The art of deception: Controlling the human element of security.* Indianapolis, Indiana, USA: Wiley Publishing, Inc.

Sasse, M. A., Brostoffand, S. i Weirich, D. (2001). Transforming the 'weakest link' - a human/ computer interaction approach to usable and effective security. *BT Technology Journal, 19,* 122-131.

Selmar, M. i Tibert, V. (2018). Reducing consumer risk in electronic marketplaces. *Computer in Human Behavior, 86,* 205-217.

Starčević, V. (2018). Problematic Internet use, reward sensitivity and decision making. *Australian and New Zaeland Journal of Psychology, 49,* 937-938.

Šolić, K. i Ilakovac, V. (2009). Security perception of a portable PC user (The difference between medical doctors and engineers): a pilot study. *Medicinski Glasnik Ljekarske komore Zeničko-dobojskog kantona, 2,* 261-264.

Šolić, K., Ilakovac, V., Marusic, A. i Marusic, M. (2009). Trends in using insecure e-mail services in communication with journal editors. *Proceedings PRC*, 50.

Šolić, K., Očevćić, H. i Baležević, D. (2015). Survey on Password Quality and Confidentiality. *Automatika, 56*(1), 69–75.

Šolić, K., Velki, T. i Galba, T. (2015). Empirical study on ICT system's users' risky behavior and security awareness. *Hrvatska udruga za informacijsku i komunikacijsku tehnologiju, elektroniku i mikroelektroniku – MIPRO proceedings,* 1623-1626.

Velki, T., Šolić, K., Gorjanac, V. i Nenadić, K. (2017). Empirical study on the risky behavior and security awareness among secondary school pupils - validation and preliminary results. *Hrvatska udruga za informacijsku i komunikacijsku tehnologiju, elektroniku i mikroelektroniku – MIPRO proceedings,* 1496-1500.

Velki, T., Šolić, K. i Nenadić, K. (2015). Razvoj i validacija Upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava (UZRPKIS). *Psihologijske teme, 24*(3), 401-424.

Velki, T., Šolić, K. i Očevćić, H. (2014). Development of Users' Information Security Awareness Questionnaire (UISAQ) - Ongoing Work. *Hrvatska udruga za infor-*

macijsku i komunikacijsku tehnologiju, elektroniku i mikroelektroniku – MIPRO proceedings, 1564-1568.

Voyiatzis, A. G., Fidas, C. A., Serpanos, D. N. i Avouris, N. M. (2011). An Empirical Study on the Web Password Strength in Greece. *15th Panhellenic Conference on Informatics*, 212-216.

Wanli, M., Campbell, J., Tran, D. i Kleeman, D. (2010). Password Entropy and Password Quality. *4th International Conference on Network and System Security,* 583-587.

doc. dr. sc. Marin Vuković
Fakultet elektrotehnike i računarstva Zagreb

4. OSOBNA SIGURNOST I ZLOĆUDNI PROGRAMI NA INTERNETU

Sažetak

Zloćudni kod općeniti je naziv za računalne programe kojima je cilj na neki način naštetiti računalnom sustavu, računalu i mreži. Prvi takav kod napisan je 1971. godine kao eksperiment. Nazvan je Creeper te se smatra pretečom današnjih modernih zloćudnih programa raznih vrsta. U počecima nastanka zloćudnih programa cilj je bio zastrašiti korisnike porukom na ekranu ili, u najgorem slučaju, onesposobiti napadnuto računalo. Danas je situacija bitno drukčija, a glavni motivi su najčešće financijske prirode.

U ovome poglavlju pojašnjene su vrste zloćudnog koda te načini napada na računalne sustave korisnika te načini napada na proizvodne pogone i državne institucije. Osim metoda poput spama, phishinga, društvenog inženjeringa, ransomwarea i botneta, obrazlažu se načini i razlozi špijunaže te cyberratovanja.

U današnje vrijeme pojedinac nikako ne smije zanemariti prijetnju zloćudnih programa pametnim telefonima jer je sve više zloćudnih programa usmjereno na pametne telefone. Pametni telefoni su široko dostupni, sve se više koriste, a korisnici ih još uvijek ne shvaćaju kao moćne uređaje na kojima se, uz korisne aplikacije, može izvoditi i zloćudni kod.

Korisnike od zloćudnih programa prvenstveno štite antivirusni programi. Međutim, korisnici trebaju biti svjesni da rizik uvijek postoji te biti oprezni u korištenju svih vrsta računalnih sustava. Najbitnije je ne nasjedati na ponude besplatnih sadržaja, programa i medija, koje mogu preuzeti s ilegalnih servisa kao što je torrent ili sa ilegalnih mrežnih sjedišta koja nude besplatne inačice programa i alata.

4.1. KRATKA POVIJEST I GLAVNE ZNAČAJKE ZLOĆUDNIH PROGRAMA

Zloćudni kod (engl. *malware*) općeniti je naziv za računalne programe kojima je cilj naštetiti računalnom sustavu na kojemu su pokrenuti. Prvi takvi programi kreirani su eksperimentalno, ne nužno sa zloćudnom namjenom. Kao prvi zloćudni kod navodi se program Creeper iz 1971. godine koji je, nakon pokretanja na računalu, ispisivao poruku korisnicima (Wikidot). Specifičnost Creepera jest da se samostalno širio i pokretao na računalima u lokalnoj, tada vrlo ograničenoj, mreži. Naziv „*virus*", koji je još uvijek često korišten, uveden je početkom 80-ih godina dvadesetog stoljeća kada su zloćudni programi polako počeli postajati prijetnja računalnim sustavima.

Neki od poznatijih prvih virusa, koji su utrli put modernim zloćudnim programima, su Jerusalem (MalwareWiki, 2017), specifičan po tome da se aktivirao na petak 13. i brisao sve podatke te Michelangelo koji se aktivirao 3. ožujka (rođendan poznatog Michelangela) i također brisao podatke korisnika (TrendMicro, 2017). Uz to, zloćudni kod Michelangelo je specifičan i po tome da se pokretao na nižoj razini računala od prethodnih virusa – umjesto pokretanja na razini operacijskoga sustava, Michelangelo se izvodio na razini tzv. *Master Boot Record*a, odnosno upravljačkog BIOSa.

Vremenom su se razvijale nove inačice zloćudnih programa sa sve naprednijim funkcionalnostima koje su svakako postajale sve zlonamjernije. Neki od tadašnjih virusa pokušavali su u potpunosti onesposobiti računalo na kojem su pokrenuti, pa je u tom smislu izmišljen i termin „*bricking*" što bi u slobodnom prijevodu značilo pretvaranje računala u ciglu, odnosno beskorisnu kutiju. Međutim, danas to više nije slučaj, jer svako računalo, poslužitelj, pametni telefon ili bilo koji drugi zaraženi uređaj predstavlja potencijal za daljnje napade zbog svoje procesorske moći. Tako da se današnji zloćudni programi više usmjeravaju na pretvaranje računala u sredstvo kojim napadač može izvoditi daljnje napade ili pak zahtijevati otkupninu od korisnika kako bi uklonio zloćudni program.

Možda i najzanimljivija osobina zloćudnih programa je način na koji se šire, jer je širenje zapravo jedini način za nanošenje dugoročne i veće štete korisnicima i računalnim sustavima. Već prvi zloćudni programi mogli su se samostalno širiti mrežom, no razlog tome bio je više eksperimentalne prirode i bili su namijenjeni zatvorenim mrežama jer u to doba nije postojao internet kakav danas poznajemo. Prvi doista zlonamjerni programi napravljeni su tako da se šire prijenosnim medijima, kao što su diskete, koje su u ondašnje vrijeme bile najraširenij način prijenosa podataka između računala. Zloćudni program bi se kopirao na disketu zajedno s korisnim podatcima te bi se na odredišnom računalu pokrenuo

i izvršio svoju namjenu. Iz tog su razloga već u 90-im godinama napravljeni prvi antivirusni programi koji su nadzirali sve datoteke koje se nalaze na računalu i sve prijenosne medije koji donose podatke u sustav. Od nastanka prvih antivirusnih alata do danas traje svojevrsno natjecanje antivirusnih tvrtki i zlonamjernih pojedinaca i organizacija u tome kako otkriti zloćudni kod, odnosno kako napraviti zloćudni kod koji se neće moći otkriti.

Kako bismo bolje shvatili zloćudni kod i ciljeve, potrebno je razraditi motivaciju zloćudnog pojedinca ili organizacije za izradom takvih programa, čime se bavi sljedeće poglavlje. Nakon toga su izložene podvrste zloćudnog koda, prvenstveno na temelju načina širenja i funkcionalnosti koje se izvode na zaraženom sustavu ili računalu. Konačno, na kraju su opisani načini zaštite te preporuke za korisnike u smislu zaštite vlastitih sustava i podataka.

4.2. ZAŠTO POSTOJE ZLOĆUDNI PROGRAMI?

Kako bi se shvatile funkcionalnosti pojedinih zloćudnih programa potrebno je razmotriti općenitu motivaciju za izradu zloćudnog koda. Kako je navedeno, cilj prvih zloćudnih programa bio je zastrašiti korisnike porukom na ekranu ili, u najgorem slučaju, onesposobiti napadnuto računalo. Danas je situacija bitno drukčija, a glavni motivi su najčešće financijske prirode.

Internet je najveća svjetska mreža s ogromnim brojem korisnika koji je koriste za zabavu, ali i informiranje o proizvodima, kupovinu i različite transakcije. Posljedica toga je da se na našim računalima i u okviru internetskih usluga, u tzv. oblaku (engl. cloud), nalazi značajna količina naših osobnih i manje osobnih podataka. Podatci o nama, našim navikama i interesima, a posebice brojevi naših kreditnih kartica, telefonski brojevi i slični osobni podatci, potencijalnim napadačima omogućuju stvaranje slike o nama i iskorištavanje tih podataka protiv nas ili naših prijatelja i kolega. U nastavku je dano nekoliko primjera ilegalne zarade na internetu koji predstavljaju dobar motiv za izradu zloćudnog koda.

4.2.1. SPAM PORUKE

Svi smo upoznati s tzv. *spam* porukama u elektroničkom sustavu. Najčešće su to reklame za proizvode koji nas ne zanimaju, a filteri naših e-sandučića više ili manje uspješno ih uklanjaju. No, takve poruke se temelje na količini poslanih poruka. Ako napadač ima pristup ogromnom broju postojećih e-adresa , nije problem poslati reklamu na tisuće i tisuće osoba i poduzeća. Ukoliko samo mali postotak primatelja uistinu otvori poruku i zainteresira se za proizvod, tzv. *spam* kampanja može ipak biti uspješna. U pozadini svega je neko poduzeće koje na

taj način reklamira svoj proizvod i spremno je napadaču platiti određenu svotu kako bi dosegla određen broj korisnika. S druge strane, napadač se reklamira poduzeću s obećanjem da će njihova reklamna poruka doseći određen broj korisnika i za to traži određeni iznos. Kada sagledamo veličinu interneta, postaje jasno da napadači i od ovakvih, naizgled bezazlenih napada, mogu imati značajnu financijsku korist.

Ono što je zanimljivo u kontekstu zloćudnog koda jest: kako je napadač došao u posjed svih tih postojećih e-adresa? Česti odgovor je upravo – zloćudni kod. Zamislimo da je napadač napravio zloćudni kod koji će nakon zaraze korisničkoga računala ili mrežne usluge za slanje poruka iščitati sve e-adrese s kojima je korisnik komunicirao. Sve te adrese su valjane adrese i napadač može biti siguran da će njegova poruka doista doći do pravog korisnika. Prikupljanje adresa je osobina gotovo svih današnjih zloćudnih programa. Nekada je motiv samo *spam* (reklamne poruke putem elektroničke pošte), no češće se radi o tome da se, uz *spam* i ostale napade, adrese koriste i za daljnje razašiljanje samog zloćudnog koda, kako bi se na isti način prikupilo još više stvarnih e-adresa.

4.2.2. DRUŠTVENI INŽENJERING I PHISHING

Zamislimo da je napadač doista dobio pristup našim kontaktima. Jednostavniji način jest da pokuša na sve te kontakte poslati *spam* poruke u nadi da će netko doista i otvoriti reklamnu poruku. Inteligentniji i puno uspješniji način jest da napadač kontaktira naše kontakte s lažiranom adresom pošiljatelja i navede naše kontakte na mišljenje da im tu poruku šaljemo mi. Tehnički je to dosta jednostavno izvedivo, ukoliko se ne koristi infrastruktura javnog i privatnog ključa popraćena certifikatima. Naši kontakti će tada puno lakše otvoriti poruku i reagirati na upute iz poruke. Slanje poruka u kojima napadač pokušava navesti primatelja na neku akciju naziva se *phishing*, a postupak u kojem se te poruke personaliziraju primateljima na temelju ukradenih podataka (u ovom slučaju samo adrese pošiljatelja) – društveni inženjering.

Treba svakako naglasiti da je društveni inženjering puno širi pojam od *spam* poruka i napadačima otvara puno više mogućnosti, zavisno o količini osobnih podataka koje je napadač uspio prikupiti o osobi. Postoje primjeri lažnih poruka u kojima se tražila otkupnina za navodne otmice, a preduvjet za takve poruke bilo je poznavanje obiteljskih prilika i odnosa žrtava kako bi napadači mogli stvoriti priču o navodnoj otmici. U svakom slučaju, društveni inženjering danas je vjerojatno i najopasniji vektor napada jer omogućuje značajnu personalizaciju i otvara put nebrojenim prevarama na internetu. Ponavljamo, uloga zloćudnog

koda jest upravo provala u sustave i računala te prikupljanje tih osobnih podataka na temelju kojih se izgrađuje prevara.

Drugi pojam koji je potrebno naglasiti jest *phishing*. Kako smo naveli, on označava slanje poruke korisniku, odnosno žrtvi, kako bi ga naveo na neku akciju. *Phishing* je bitan zato što se upravo pomoću njega izvodi najveći broj prevara i gotovo uvijek predstavlja prvi vektor, odnosno korak napada. Ukoliko korisnik nasjedne na taj prvi korak, napadaču se otvaraju mogućnosti za daljnje napade i akcije koje imaju za cilj kompromitaciju podataka ili sustava korisnika.

Najtipičniji primjer *phishinga* je poruka u kojoj se primatelja navodi na promjenu lozinke na nekoj usluzi zbog nekog izmišljenog razloga. Ukoliko žrtva povjeruje poruci, poveznica je vodi na lažiranu internetsku stranicu koja izgleda kao stvarna forma za unos podataka za prijavu. Unosom, primjerice, imena i zaporke, žrtva ih zapravo predaje napadaču koji nadalje može pristupati ciljanoj usluzi sa svim ovlastima žrtve. Uz to, žrtva toga često nije niti svjesna. Nakon toga napadač račun žrtve koristi za daljnje napade s lažnim identitetom žrtve. Nedavni primjer ovakvog napada napravljen je korisnicima usluge Gmail, gdje su napadači nakon krađe podataka za pristup svim kontaktima žrtve slali poruke o navodnoj potrebi za financijskom pomoći zbog problema u inozemstvu.

Kao i kod *spam* poruka, navedene metode i primjeri u konačnici imaju za cilj napadaču osigurati financijsku dobit, u ovom slučaju na nešto složeniji, ali i isplativiji način.

4.2.3. KOMPROMITIRANI UREĐAJI KAO DIO BOTNETA

Do sada razrađena motivacija za izradu zloćudnog koda uključivala je, u pravilu, prikupljanje podataka koji napadačima pomažu u provedbi daljnjih napada. Međutim, ako razmatramo slanje *spam* ili *phishing* poruka, potrebno se zapitati od kuda se šalju te poruke. Kako bi napadač mogao poslati puno poruka u kratkom vremenu, potrebna mu je infrastruktura koja se sastoji od mnoštva računala koja mogu obrađivati podatke i slati, u danom primjeru, zlonamjerne eporuke. Zato je posljednjih godina čest trend u kojemu se zloćudni kod zadržava na računalu ili sustavu žrtve kako bi napadač mogao kontrolirati to računalo i koristiti ga, u ovom primjeru, za slanje poruka. Nakon zaraze korisničkog računala, napadač ga može kontrolirati pomoću naredbi i pokretati različite scenarije napada. U tom kontekstu važan je pojam tzv. kontrolnog poslužitelja (*command and control server, C&C*) s kojeg napadač šalje naredbe svim zaraženim računalima. Mreža zaraženih računala naziva se botnet, a zaraženo računalo koje je dio te mreže *bot*.

Iako problematika *botneta* izlazi iz okvira razmatrane uloge zlćudnih programa, potrebno je napomenuti kako *botneti* služe i za druge maliciozne aktivnosti izuzev slanja *spam* ili *phishing* poruka. Posljednjih godina zabilježen je trend gdje se zaražena računala koriste za napade na infrastrukturu interneta, primjerice poslužitelje usluge DNS (*Domain Name Service*), kako bi se onemogućio pristup uslugama za dio ili cijelu mrežu. U tom slučaju *botnetovi* predstavljaju veliku opasnost koja nadilazi zlonamjerne poruke jer mogu ugroziti čitavo funkcioniranje interneta.

Napadači koji upravljaju velikim *botnetovima* od njih mogu imati veliku financijsku dobit upravo zbog mogućnosti napada s velikog broja računala u različitim mrežama, pa je jedna od čestih primjena botneta distribuirani napad uskraćivanjem usluge (*Distributed Denial of Service, DDOS*). Uspješan DDOS će ciljanu uslugu na neko vrijeme učiniti u potpunosti nedostupnom, što može biti zanimljivo konkurenciji, pa je jasno zašto napadači od toga mogu imati financijsku korist.

Podsjetimo, zlćudni kod pokrenut na računalu žrtve je preduvjet i za napade ove vrste, pa je motivacija za izradu takvog koda i u ovom slučaju jasna.

4.2.4. NAPLATA OTKUPNINE OD ŽRTVE

Ova vrsta ugroze postala je vrlo raširena u posljednjih nekoliko godina i većinom je usmjerena na osobna računala korisnika iako postoje i verzije razvijene za pametne telefone. Zlćudni programi ove vrste nazivaju se *ransomware,* a cilj im je šifriranje podataka na korisničkom računalu kako im korisnik više ne bi mogao samostalno pristupiti. Jednom šifrirane podatke nemoguće je dešifrirati bez odgovarajućeg ključa za šifriranje koji je u vlasništvu napadača. Nakon šifriranja, napadač kontaktira žrtvu te traži otkupninu za podatke, kako bi žrtvi otkrio ključ za dešifriranje. Naravno, plaćanjem otkupnine nema garancija da će napadač uistinu žrtvi i otkriti ključ i da će žrtva doista moći vratiti svoje podatke.

Kao i kod prethodnih primjera, *ransomware* se većinom prenosi putem poruka, najčešće e-poštom, gdje se metodama *phishinga* pokušava žrtvu natjerati da pokrene zlćudni kod koji joj je poslan kao privitak poruke. Ukoliko žrtva nije na oprezu, pokrenut će privitak koji će instalirati zlćudni program na računalo. Privitci u kojima se nalazi zlćudni kod ne moraju biti izvršne datoteke (npr. .exe) nego često iskorištavaju postojeće ranjivosti drugih alata na računalu. Primjerice, čest je slučaj gdje se zlćudni kod šalje kao dio datoteke PDF. Prilikom pokretanja, alat za pregled dokumenta u formatu PDF učitava dokument i pritom, zbog vlastitih ranjivosti, izvrši zlćudni kod koji se nalazi prikriven u dokumentu PDF.

Uz navedene korake napada, treba naglasiti i da napadači često koriste metode društvenog inženjeringa, pa tako primjerice računovodstvene odjele tvrtki zasipaju e-poštom koja sadrži privitke koji izgledaju kao računi, čime se povećava vjerojatnost da će žrtva doista otvoriti privitak i pokrenuti zloćudni kod.

4.2.5. ŠPIJUNAŽA

Danas je većina poslovanja tvrtki u potpunosti digitalizirana i nalazi se na poslužiteljima u lokalnoj mreži ili, djelomično, u dijeljenom oblaku. Zaposlenici tvrtke, ovisno o ovlastima, imaju određeni pristup povjerljivim dokumentima i podatcima nužnim za poslovanje tvrtke. Ako napadač može ostvariti pristup samo jednom računalu zaposlenika, potencijalno može kompromitirati cijelu mrežu poduzeća.

Primjerice, zamislimo tvrtku koja se bavi proizvodnjom i određeni zaposlenici uključeni su u dizajn novih proizvoda i patentiranja. Konkurentsko poduzeće dobilo bi veliku tržišnu prednost ako bi mogla doći u posjed dokumentacije i patentnih prijava novih proizvoda. Ukoliko napadač može doći do takvih podataka, razumljivo je zašto bi mu konkurentska tvrtka htjela platiti informacije, pa je opravdan motiv napadača za provalom u takve, poslovne sustave. Kao i kod ostalih vrsta zloćudnih programa, i ovdje je najčešći prvi korak slanje *phishing* poruke koja sadrži zloćudni kod i tipično uključuje metode društvenog inženjeringa. Nakon instalacije zloćudnog koda na računalo žrtve, napadač dobiva ovlast žrtve i može pristupati svim informacijama kao i žrtva.

Kroz godine je zabilježeno podosta slučajeva industrijske špijunaže prema navedenim obrascima, no poduzeća često ne žele potvrditi takve napade kako bi sačuvale ugled. Ipak, postoje primjeri u kojima su na ovaj način, navodno, napadači iz Kine ili Sjeverne Koreje provaljivali u sustave tehnoloških tvrtki iz Japana kako bi došli do korisnih poslovnih informacija.

4.2.6. CYBER RATOVANJE

Najsloženiji zloćudni programi napravljeni su kako bi se špijunirale druge države i sustavi ili nanijela šteta industrijskim i vojnim sustavima od kritične važnosti. Iako je potvrđeno postojanje ovakvih složenih zloćudnih programa, nikada nisu potvrđeni autori niti tko ih je financirao, što je očekivano s obzirom na razinu i ciljeve takvih programa. Pretpostavka je da su ih razvili specijalizirani timovi koji rade za države s obzirom da se troškovi razvoja takvih programa procjenjuju u milijunima dolara, a indikativne su i mete koje takvi programi ciljaju.

Najpoznatiji primjer takvog zloćudnog programe jest crv Stuxnet (Holloway, 2015), koji je bio najsloženiji zloćudni program u povijesti. Napravljen je da po lokalnoj mreži pronalazi Siemensove kontrolere u proizvodnom pogonu te preuzme kontrolu nad njima kako bi onesposobio ili potpuno uništio fizičku infrastrukturu kojom se njima upravlja. Indikativno je to da su se Siemensovi kontrolori koristili u nuklearnim pogonima Irana i da je na te pogone izveden uspješan napad korištenjem upravo crva Stuxnet, pa se može samo pretpostavljati tko stoji iza razvoja. Nakon Stuxneta razvijeno je još nekoliko naprednijih i manje naprednih izvedenica koje su imale za cilj špijunažu, no do danas nisu potvrđeni autori. Zanimljivo je da je jedna izvedenica i ove 2018. godine otkrivena na poslovnoj mreži poznate antivirusne tvrtke Kaspersky Labs (Kaspersky Labs), koja je dulje vremena uopće nije primijetila.

Vektori napada kod ovakvih vrsta zloćudnoga koda su različiti, iako ponovno prednjači metoda *phishinga* uz društveni inženjering. Kod ovakvih složenih programa, nakon inicijalne zaraze jednog računala u lokalnoj ili štićenoj mreži, zloćudni programi se dalje sami šire mrežom i na taj način dolaze do novih računala s traženim podatcima ili upravljačkim sklopovljem. Primjerice, po nekim izvorima, pretpostavlja se da Stuxnet nije pokrenut u iranskom nuklearnom pogonu *phishingom*, već da se nalazio na USB memoriji koju je netko ostavio blizu nuklearnog pogona. Žrtva je tada uzela USB memoriju i uključila je u računalo u zaštićenoj mreži, kako bi provjerila podatke na memoriji. No, već nakon uključivanja memorije u računalo, Stuxnet je pokrenut i mogao se dalje samostalno širiti mrežom u potrazi za Siemensovima kontrolorima.

4.2.7. NAPLATA SMS PORUKA ZA USLUGE S DODANOM VRIJEDNOSTI

Dosadašnji primjeri uglavnom su se usmjeravali na računala i sustave, no nikako se ne smije zanemariti prijetnja zloćudnih programa pametnim telefonima. Zapravo, posljednjih nekoliko godina razvija se više zloćudnih programa za pametne telefone nego za tradicionalna računala. Pametni telefoni su široko dostupni, godinama se sve više i više koriste, a korisnici ih još uvijek ne shvaćaju kao moćne uređaje na kojima se, uz korisne aplikacije, može izvoditi i zloćudni kod.

Napadačima su pametni telefoni zanimljivi jer imaju nekoliko specifičnosti u usporedbi s računalima. Prije svega, tu je mogućnost izravne naplate telekom operatora pa napadač može vrlo brzo doći do financijske koristi. Najčešći primjer zarade jest slanje SMS poruka za usluge s dodanom vrijednosti koje su u izravnom ili neizravnom vlasništvu napadača. Na taj način napadač koristi pametni telefon žrtve kako bi u pozadini slao SMS poruke na vlastitu uslugu i time zarađivao novac, žrtva uopće nije svjesna slanja poruka. Tipičan scenarij za

ovakvu ranjivost jest da napadač iskoristi postojeću, legitimnu, aplikaciju u koju ubacuje dio programskog koda za slanje SMS poruka svojoj usluzi. Uobičajeno će napadač preuzeti legitimnu aplikaciju s neke od trgovina aplikacija, provesti proces reverznog inženjerstva kako bi došao do izvornog koda aplikacije i u taj kod ubaciti svoj maliciozni dio koda. Nakon toga se aplikacija ponovno pakira i nudi korisnicima besplatno putem ilegalnih trgovina ili sličnih mehanizama za dijeljenje sadržaja (npr. servisi *torrent*). Korisnicima je primamljiva činjenica da je ta aplikacija sada besplatna, dok bi je na legitimnoj trgovini trebali kupiti. Zato pristaju na preuzimanje neprovjerene aplikacije s alternativnih izvora čime se dovode u ugrozu. Po instalaciji takve aplikacije korisnici je mogu normalno koristiti, no nisu svjesni da aplikacija tijekom korištenja iz pozadine šalje skupe SMS poruke na napadačevu uslugu. Danas je ovakva vrsta ugroze dominantna na uređajima s operacijskim sustavom Android, dok je prvi zabilježeni slučaj ovakvog zloćudnog koda zabilježen kod operacijskog sustava *Symbian* u obliku igre *Mosquito* (Peikari, Fogie, Read i Hettel, 2004) 2007. godine.

Uz izravnu naplatu putem pametnih telefona, ne treba zanemariti ni činjenicu da pametni telefoni o nama prikupljaju velike količine podataka kao što su navike u kretanju, korištenju telefona, kontaktima, čestim lokacijama koje posjećujemo i slično, pa kao takvi napadačima predstavljaju dobar izvor osobnih podataka o korisnicima. Dodatna mogućnost je i instalacija zloćudnih programa čiji je cilj nadzor uređaja i drugih aplikacija na pametnom telefonu kao što su bankarske aplikacije ili aplikacije za komunikaciju, koje otvaraju put za daljnje napade i financijsku korist napadačima. Za očekivati je da će se broj prijetnji na pametnim telefonima i dalje povećavati te da će prijetnje postajati sve složenije pa je potrebno obratiti pozornost na izvore iz kojih se aplikacije preuzimaju.

4.3. VRSTE ZLOĆUDNOG KODA

Zloćudni programi se vremenom mijenjaju kako bi mogli ostati neotkriveni antivirusnim alatima. Međutim, postojeće zloćudne programe moguće je klasificirati prema funkcionalnostima i načinu širenja. Pri tome treba reći da se neki primjeri ne mogu jednoznačno klasificirati jer se, zbog evolucije, šire na više načina, a ovisno o namjeni mogu imati i različite funkcionalnosti.

Prema tome, zloćudne programe možemo dijeliti na sljedeće kategorije s navedenim glavnim značajkama:

- računalni virusi - ne šire se samostalno između računala,
- računalni crvi - šire se samostalno između računala,

- trojanski konji - predstavljaju se kao korisni programi,
- *rootkitovi* - napadaču omogućuju kontrolu nad cijelim sustavom žrtve,
- *ransomware* - šifriraju podatke žrtve,
- *spyware* - nadziru aktivnosti žrtve,

4.3.1. RAČUNALNI VIRUSI

Računalni virusi su vrsta zloćudnog koda koji se samostalno izvršava kako bi nanio štetu sustavu na kojemu se pokreće. Virusi se često ugrađuju u legitimne datoteke kako bi se pokrenuli kada korisnik pokrene i datoteku, primjerice sliku, dokument u formatu PDF ili .doc. Često se dodaju na početak ili kraj legitimne datoteke kako bi se neprimjetno pokrenuli, pa će se tako virus izvršiti, a ostatak legitimne datoteke će se korisniku uobičajeno prikazati kako on ne bi posumnjao na moguću zarazu.

Glavno svojstvo virusa je da se, nakon prvog pokretanja, sami pokušavaju replicirati unutar računala ili sustava na kojima su pokrenuti, no u pravilu se ne šire samostalno između računala. Replikacija se može provesti tako da virus prije svega utvrdi na kojem je operacijskom sustavu pokrenut, pa prema tome „zna" koje sve datoteke postoje i gdje se sve može ubaciti. Nadalje pretražuje sustav s poznatim datotekama i redom se dodaje u njih kako bi se zaraza proširila. Ovisno o metama virusa, postoji nekoliko podvrsta koje su opisane u nastavku.

Prva i najstarija vrsta su virusi koji ciljaju datotečni sustav. Takvi će se virusi ubacivati u sve datoteke kako je opisano. Poseban problem je da ako takvi virusi dospiju u memoriju računala, tada se mogu zapisati u svaku izvršnu datoteku koja se pokreće i na taj se način mogu širiti i na ostale programe koji se izvode na napadnutom računalu. Primjer jednog od prvih ovakvih virusa je Jerusalem (MalwareWiki, 2017).

Sljedeća vrsta su virusi koji se ubacuju u *boot* sektore računala. *Boot* sektori su dio memorije, odnosno diska računala koji se učitavaju u memoriju pokretanjem računala i očitavanjem vanjskog medija, kao što je USB memorija. Oni prilikom pokretanja daju uputu sustavu koje programe treba učitati u memoriju. Ako se virus ubaci u boot sektor, to znači da će se on učitati u memoriju računala kod pokretanja, čime će biti u stanju nanijeti znatno veću štetu i bit će ga teže ukloniti. Kao primjer prvog ovakvog virusa navodi se Michelangelo. Svojevrsna nadogradnja virusa u *boot* sektorima su virusi u glavnom *boot* zapisu (*Master Boot Record, MBR*), kojim se određuje kako će se pokrenuti računalo i iz kojih *boot* sektora će se podizati sustav i programi. Takvi su virusi u stanju nanijeti još veću štetu jer će moći utjecati na pokretanje ostalih programa ili učitavanje

čitavih diskovnih particija računala. Jedan od najstarijih primjera MBR virusa je NYB (Symantec, 2000).

Posljednja općenita vrsta virusa su višepartitni virusi. Nazivaju se tako jer se ne ograničavaju samo na datoteke ili samo *boot* sektore, već se pokušavaju replicirati i u datotečni sustav i u *boot* sektore. Zbog toga ih je posebno teško ukloniti, jer će se brisanjem virusa iz datotečnog sustava zaraza ponovno proširiti iz *boot* sektora ili MBR i obratno. Primjer ovakvog virusa je Tequilla (FSecure, 2018).

Uz navedene općenite vrste virusa, možda i najčešća specifična vrsta su makro virusi (engl. macro). Pojam makro označava automatizaciju datoteka paketa Microsoft Office, kao što su Word, Excel, Powerpoint i Access dokumenti. U odgovarajućim alatima su ugrađene funkcionalnosti koje korisnicima omogućuju pisanje naredbi i koda kako bi se olakšao rad s tim dokumentima. Međutim, u alatima su otkrivene i otkrivaju se određene ranjivosti pa je umjesto legitimnih naredbi moguće ubaciti zlonamjerni kod koji će se izvršiti pokretanjem odgovarajućeg dokumenta. Pri tome će kod imati ovlast programa koji ga je pokrenuo pa će takav makro virus moći napraviti značajnu štetu i izvan okvira alata paketa Microsoft Office. Jedan od najpoznatijih makro virusa je W97M.Melissa (Panda Security, 2013).

Govoreći o računalnim virusima, treba spomenuti i svojstvo polimorfizma. Naime, antivirusni alati, o kojima će biti više riječi kasnije u tekstu, zloćudne programe otkrivaju na principu „otiska". Svaki zloćudni program imat će jedinstven „otisak" koji će odgovarati zapisu izvršnog zloćudnog koda. Postojanjem baze takvih otisaka, antivirusni program će u datotečnom sustavu i memoriji računala pretraživati pojavu poznatih otisaka kako bi utvrdio prisutnost zloćudnog programa. Zato je važno svojstvo polimorfizma, kod kojeg će zloćudni program replikacijom mijenjati svoj kod kako bi ga bilo teže detektirati. Danas su gotovo svi virusi polimorfni u ovom smislu i to je jedan od razloga zašto treba redovito ažurirati antivirusne programe koji tada preuzimanju nove „otiske" izmijenjenih virusa. Vezano uz prikrivanje virusa, čest je slučaj i da virusi odmah nakon pokretanja pokušavaju detektirati postoji li na računalu antivirusni program i koje je vrste. Ukoliko postoji, virus će ga pokušati deaktivirati i to često na način da izgleda kao da je antivirusni program pokrenut i ispravan kako korisnik ne bi posumnjao na zarazu.

4.3.2. RAČUNALNI CRVI

Računalni crvi su zloćudni programi čija je glavna karakteristika da se mogu samostalno širiti mrežom. Izuzev načina širenja, u ostali segmentima su vrlo slični računalnim virusima, pa se u nekim kategorizacijama navode i kao pod-

vrsta virusa. No, za razliku od virusa, crv se ne ubacuje u datoteku kako bi ga korisnik ili sustav pokrenuo, već ima vlastite mehanizme širenja koji ne ovise o izvanjskim akcijama. Upravo zbog te samostalnosti su možda i najopasnija vrsta zloćudnog koda jer su u stanju brzo preplaviti i zaraziti velik broj računala u mreži. Gledajući unazad, treba reći da prvi crvi nisu razvijeni s malicioznim namjerama, već na temelju ideje da se omogući automatizirano ažuriranje programa na računalima. Tako bi se „legitimni" crv pustio u mrežu u kojoj bi sam tražio računala sa starijom verzijom nekog programa, pokrenuo se na takvim računalima i ažurirao program.

Proces širenja crva je sljedeći. Slično kao i virus, crv prvo detektira sustav na kojem se nalazi i pokušava iskoristiti poznate ranjivosti. Nakon uspješnog iskorištavanja ranjivosti počinje se replicirati i tražiti nove mete. Nove mete pronalazi u kontaktima elektroničke pošte, popisu računala u lokalnoj mreži, tablicama usmjeravanja ili čak slučajno generiranim IP adresama. Prema načinima širenja moguće je razlikovati crve (Symantec, 2016):

- *e-mail* crvi – šire se elektroničkom poštom, najčešće kao privitak. Uz to, eventualno se koriste i metode društvenoga inženjeringa kako bi meta vjerovala pošiljatelju i lakše otvorila privitak s crvom,
- internetski crvi – pretražuju mrežu kako bi identificirali računala s poznatim ranjivostima (npr. identifikacijom verzije operacijskog sustava) i otvorenim vratima, te na taj način ulaze u druga računala,
- mrežni crvi – pronalaze dijeljenu pohranu (npr. mrežne diskove, pohranu mrežnog pisača i slično) na koju se kopiraju.

Bez obzira kako su mete pronađene, odgovarajućim kanalom se metama šalju paketi koji ponovo sadrže crva čime cijeli postupak počinje ponovo.

Osim širenja, glavna funkcionalnost crva jest nanošenje štete računalu na kojemu je pokrenut. Tu je crv vrlo sličan virusu, pa tako može brisati ili mijenjati datoteke, prikupljati različite dostupne informacije o korisniku ili, u najgorem slučaju, preuzeti računalo i omogućiti napadaču potpunu kontrolu otvaranjem sustava kroz tzv. *backdoor*. Ukoliko se otvori takav ulaz u računalo, ono postaje dio napadačevog *botneta* i kasnije može biti iskorišteno za različite vrste napada, primjerice napade uskraćivanjem usluge, slanje *spam* poruka ili korištenje procesorskih resursa računala. Posljednje je posebno zanimljivo jer postoje i legitimni programi kojima korisnik može dopustiti korištenje vlastitih resursa, primjerice projekt SETI@home (https://setiathome.berkeley.edu, preuzeto 15.10.2018.). U kontekstu zloćudnih crva, s rastom popularnosti virtualne valute Bitcoin napravljeni su crvi koji su se pokretali na računalima i rudarili Bitcoinove kako bi napadaču osigurali financijsku dobit.

Uz sve navedeno i s obzirom na činjenicu da su crvi doista najnapredniji zloćudni programi, treba razmisliti i o problemima na koje crvi nailaze. Prije svega, njihovo agresivno širenje mrežom može biti i loše za njih, jer postavlja se pitanje - kako spriječiti da crv „prepiše" sam sebe, odnosno više puta zarazi isto računalo? Očigledno, moraju postojati mehanizmi za kontrolu je li crv već pokrenut na nekom računalu, što može biti složeno ukoliko je cilj crva da ga bude teško otkriti, čak i „vlastitoj kopiji". Uz to, složeni crvi moraju sadržavati programsku logiku koja će moći detektirati ranjivosti, kao i logiku potrebnu za širenje unutar i izvan računala. Zbog svega toga postoji mogućnost da crv jednostavno postane prevelik, čime bi se otežalo širenje i olakšala detekcija, a takav crv izgubio smisao.

U nastavku su izloženi važniji primjeri računalnih crva kako bi se pojasnile njihove specifičnosti.

Vjerojatno prvi crv je Morris Worm (Bortnik, 2013) kojeg je napisao student Sveučilišta Cornell Robert Tappan Morris i pokrenuo ga 2.11.1988. godine. Prema autoru, cilj izrade crva bio je mjerenje veličine interneta. Međutim, problem je bio u mehanizmu širenja jer crv nije ispravno provjeravao je li već pokrenut na računalu, pa se više puta pokretao na istom računalu što je u konačnici rezultiralo uskraćivanjem usluge. S obzirom da je crv zahvatio veći broj računala i poslužitelja, slučaj je dobio i sudski epilog u kojem je autor osuđen. Šteta koju je Morris Worm napravio procijenjena je na 1 do 10 milijuna dolara, a prema izvještajima inficirao je 10% računala s operacijskim sustavom Unix spojenih na internet i oko 2000 računala u prvih petnaest sati od pokretanja.

Povijesno gledano, jedan od prvih crva koji je počinio štetu na globalnoj razini je Nimda (Ducklin, 2011), otkriven 2001. godine i vjerojatno napravljen u Kini. Budući da je koristio više metoda širenja, vrlo brzo se proširio mrežom. Jedan je od prvih koji se mogao pokrenuti bez da korisnik otvori poruku elektroničke pošte u kojoj se nalazio i prvi koji je modificirao web stranice da nude njegove kopije za preuzimanje. Općenito, to je jedan od najrazornijih računalnih crva ikad otkrivenih, u svakom slučaju prvi takve vrste. Napadao je operacijski sustav Microsoft Windows i širio se na sljedeće načine: e-poštom, preuzimanjem s mrežnih stranica, lokalnom mrežom pomoću dijeljene memorije, iskorištavajući ranjivosti MS IIS servera ili preko *backdoora* kreiranog od strane drugih crva - Code Red i Sandworm. Kada se jednom pokrenuo na računalu, inficirao je datoteke slično kao i virus, ali se nije dodavao u izvršne datoteke nego se kopirao s imenom izvršne datoteke, a originalnu datoteku je kopirao u sebe. Kad bi korisnik pokušao pokrenuti zaraženu datoteku, prvo bi se pokrenuo crv, a zatim originalni program. Originalna verzija Nimde inficirala je gotovo 160.000 sustava. Nakon prve verzije, sve do danas, razvijene su evoluirane verzije crva Nimda

koje još uvijek mogu načiniti štetu računalima i sustavima, a mnogi noviji crvi koriste mehanizme koje je prve koristila Nimda.

Govoreći o računalnim crvima, neizbježno je spomenuti do danas najsloženiji crv - Stuxnet (Holloway, 2015) o kojem je bilo riječi u uvodnom dijelu. Otkriven je u lipnju 2010. godine i prvi je crv koji je dizajniran za napad na Siemensove programabilne logičke kontrolere (PLC). Širio se putem operacijskog sustava Microsoft Windows, a zarazom računala tražio je kontrolira li računalo na kojem se nalazi neki PLC. Pisan je u nekoliko različitih programskih jezika i neuobičajeno je velik za zloćudni program - oko pola Mb. Ukoliko računalo na kojem je pokrenut ne zadovoljava zahtjeve u smislu kontrole nekog PLC-a, crv postaje inertan i koristi mjere zaštite kako širenjem ne bi obrisao sam sebe na drugom računalu. Između ostalog, sadrži i kompleksnu funkcionalnost koja služi za slanje lažnih senzorskih signala kako se inficirani sustav ne bi isključio ako otkrije neuobičajeno ponašanje. Specifičnost Stuxneta je da je prilikom širenja na operacijski sustav Windows koristio čak četiri tzv. *zero-day* ranjivosti. *Zero-day* ranjivosti su ranjivosti koje prethodno nisu otkrivene, pa za njih ni ne postoje sigurnosne zakrpe, što ih čini vrlo rizičnima. Korištenje čak četiri takve ranjivosti kod Stuxneta, uz to prvi put u povijesti kod bilo kojeg zloćudnog programa, svakako indicira da je iza njegove izrade tim stručnjaka sa značajnim budžetom i jasnom namjerom kompromitacije PLC-ova. Zanimljivo je i da Stuxnet nije ciljao bilo koje Siemensove PLC-ove, već je imao ugrađenu kontrolu za identifikacijom samo PLC-ova na koje su povezani uređaji za pretvorbu frekvencije jednog od dva određena proizvođača. Dodatno, napadao je samo one sustave koji rade na frekvencijama između 807 i 1210 Hz. Ukoliko je tako, Stuxnet izvršava napad periodičnim mijenjanjem frekvencije na 1410 Hz, 2 Hz i 1064 Hz što utječe na rotacijsku brzinu kontroliranih motora. Iz ovog je također očigledno da je Stuxnet razvijen ciljano kako bi napadao usku skupinu uređaja kontroliranih PLC-ovima. Studija širenja pokazala je da su Iran (58.85%), Indonezija (18.22%) i Indija (8.31%) države na koje je Stuxnet najviše utjecao te je prouzročio značajnu štetu iranskom nuklearnom programu skupljajući informacije o industrijskim sustavima i uništavajući centrifuge zbog prebrzog okretanja. Prema izvještajima uništio je petinu iranskih nuklearnih centrifuga, a u procesu je inficirao 200.000 računala.

4.3.3. TROJANSKI KONJI

Trojanski konji specifični su po tome što se korisnicima predstavljaju kao legitimni i korisni programi. Od tuda i ime trojanski konj, prema drvenom konju iz grčke mitologije pomoću kojeg su Grci ušli u grad Troju. Trojanski konji najčešće se šire nekom vrstom društvenog inženjeringa, tj. ne izvršavaju se ni

ne šire samostalno. Čest je slučaj u kojemu se nekom od metoda društvenog inženjeringa korisnicima dostavi video zapis, no da bi ga otvorili moraju preuzeti „novu inačicu" programa za reprodukciju video zapisa u kojemu se zapravo nalazi zlćudni program. Nakon infiltriranja u sustav trojanski konji imaju za cilj instaliranje različitih zlćudnih funkcija, često otvaranje *backdoora* kako bi napadač dobio potpunu kontrolu nad računalom. Treba reći i da se trojanski konji ne repliciraju, kao primjerice virusi, već ih pokreće isključivo prevareni korisnik koji ih smatra legitimnim programima.

Jedan od najpoznatijih primjera trojanskog konja je Zeus, prvi puta identificiran 2007. (Kaspersky Labs, 2018). godine. Zeus je inicijalno napravljen za krađu bankovnih podataka u čemu je bio uspješan u svojoj prvoj inačici. Kao i kod ostalih zlćudnih programa, i Zeus je evoluirao pa tako danas njegove inačice služe za instalaciju *ransomware* programa.

4.3.4. ROOTKITOVI

Rootkit je tradicionalni naziv za zlćudne programe koji napadaču omogućuju potpunu kontrolu zaraženog računala. U literaturi se navode kao posebna vrsta zlćudnih programa, no iz prethodnog teksta je očigledno da postoje i virusi, crvi i trojanski konji koji imaju funkcionalnosti rootkita.

Rootkitove možemo razlikovati prema ovlastima koje imaju prilikom infiltracije u sustav. *Rootkit* korisničke razine djeluje pod ovlastima korisnika uz ostale korisničke aplikacije, dok *rootkit* jezgrene razine djeluje na najnižoj razini s najvišim privilegijama operacijskog sustava. Tako može dodavati ili mijenjati dijelove operacijskoga sustava čime se napadačima otvaraju velike mogućnosti i potpuna kontrola zaraženog računala.

Instalacija *rootkita* može se provesti korištenjem nekog drugog zlćudnog koda, kao primjerice trojanskog konja, virusa ili crva. Nakon instalacije, moguće je prikriti napad i zadržati pristup sustavu. Otkrivanje i otklanjanje *rootkita* je složeno zbog njegove mogućnosti da mijenja programe i postavke operacijskoga sustava s ciljem prikrivanja.

4.3.5. RANSOMWARE

Ransomware je vrsta zlćudnog koda koja šifrira podatke na žrtvinom računalu i traži novčanu otkupninu kako bi ih se dešifriralo. Popularnost ove vrste zlćudnih programa je porasla od kraja 2013. zbog pojave kriptovaluta koje su olakšale plaćanje otkupnine, odnosno otežale ulazak u trag napadačima. *Ransomware* djeluje na način da šifrira žrtvine podatke. Žrtva će moći dešifrirati

podatke jedino ako dobije pristup korištenom ključu za šifriranje, koji je u vlasništvu napadača. Nakon plaćanja otkupnine, napadač bi žrtvi trebao dostaviti ključ što često nije slučaj pa je upitno ima li smisla uopće plaćati otkupninu.

Ransomware se najčešće širi putem trojanskih konja koji nakon instalacije provode šifriranje i korisnicima ispisuju poruku u zaključanim podacima i upute za plaćanje otkupnine.

Jedan od prvih *ransomware* programa bio je AIDS Trojan (KnowBe4, 2018) davne 1989. godine, no zbog greške u izradi je bilo jednostavno dešifrirati podatke bez plaćanja otkupnine. Noviji primjer je CryptoLocker (Kaspersky, 2018) koji se pojavio u rujnu 2013. godine i napadao računala s operacijskim sustavom Windows šifrirajući podatke na tvrdom disku 2048bitnim RSA ključem. Specifičan je po tome da je prvi koristio valutu Bitcoin za naplatu, a procjenjuje se da je uzrokovao štetu od 27 milijuna dolara. Još jedan noviji i poznati *ransomware* je WannaCry (Palmer, 2018), napad je počeo u svibnju 2017. i trajao četiri dana, meta su mu bila računala s operacijskim sustavom Windows, šifrirao je podatke i tražio isplatu u kriptovaluti Bitcoin, a poseban je po tome što je posjedovao mehanizam kojim se mogao samostalno širiti. U medijima je dosta popraćen, pa je tako bilo objavljeno kako je uzrokovao zastoje u zračnom prometu i velike štete u industrijskim pogonima.

4.3.6. SPYWARE

Cilj *spyware* programa je, kako im ime govori, nadzor korisnika. Cilj im je neprimjetno zaraziti računalo i u pozadini pratiti što korisnik radi, koje usluge koristi i s kojim podatcima rukuje. Prikupljeni podatci nadalje se mogu koristiti za dodatne napade na korisnika ili njegov krug kontakata. Uz to, *spyware* posjeduje mehanizme za periodičko ili stalno slanje prikupljenih podataka napadaču koji mogu biti više ili manje složeni.

Što se tiče širenja, *spyware* se bitno razlikuje od virusa ili crva zato što mu često nije cilj zaraziti što više računala, već bira određene mete. Tipično se instalira pomoću trojanskoga konja koji najčešće uključuje neku vrstu društvenog inženjeringa.

Jednostavan i netipičan primjer *spyware*a su tzv. prateći kolačići za mrežna sjedišta (engl. tracking cookies). Kod njih je cilj postaviti kolačić u preglednik korisnika kako bi se pratilo koja svemrežna sjedišta posjećuje te koliko i kako ih koristi. Nešto tipičniji *spyware* će se instalirati na računalo i raditi funkciju praćenja pokreta miša i unosa na tipkovnici, pa se takvi programi nazivaju *keyloggeri*. U posljednje vrijeme zabilježen je *spyware* koji na računalu žrtve podiže

poslužitelj za udaljeno upravljanje i nadzor računala. Kako ne bi bilo zabune, postoje brojni legitimni alati za nadzor i udaljeno upravljanje računalom kao što su TeamViewer i VNC (engl. Virtual Network Computing). No, ukoliko ih napadač pokreće i koristi bez znanja korisnika putem nekog zloćudnog programa onda im je cilj svakako zlonamjeran. Primjeri takvih zloćudnih programa, prvenstveno usmjerenih na financijske institucije, su Dridex, Neverquest i Gozi (Keshet, 2017).

4.4. ZAŠTITA OD ZLOĆUDNIH PROGRAMA

Kako bi se korisnici zaštitili od zloćudnih programa, prije svega je potrebno rezimirati kojim sve kanalima zloćudni programi mogu ući u računalo. Konačni cilj zaštite jest da se svi identificirani kanali odgovarajući zaštite, što najčešće i rade antivirusni programi. Prema gornjem tekstu i analizi postojećih primjera zloćudnih programa, možemo identificirati navedene izvore zaraze:

- e-pošta - zloćudni programi tipično dolaze kao privitak pošte ili se korisnika usmjerava na mrežno sjedište s kojega se preuzima zloćudni program,
- usluge trenutnog poručivanja i kratkih poruka - kao i kod e-pošte, posebice na pametnim telefonima, poruke mogu biti upućene i nekom od usluga trenutnog poručivanja (Whatsapp, Viber, Skype…)
- društvene mreže - kompromitacijom društvenih mreža moguće je koristiti metode društvenog inženjeringa i navesti korisnike na preuzimanje trojanskih konja izravno s mrežnog sjedišta,
- prijenosni mediji - virusi se najčešće šire ovim načinom jer se mogu pokrenuti prilikom čitanja prijenosnog medija, bez intervencije korisnika,
- otvorena mrežna vrata - crvi se često šire identifikacijom otvorenih vrata na računalu,
- ranjive mrežne usluge na računalu - crvi skeniraju računala kako bi identificirali zastarjele verzije usluga na računalu koje onda iskorištavaju za zarazu,
- preuzimanjem i instalacijom neprovjerenih programa s interneta - na računalima i pametnim telefonima, ukoliko nema verifikacije proizvođača.

Većinu navedenih kanala mogu nadzirati antivirusni programi. Tako će kvalitetni programi nadzirati sve poruke koje korisnik dobiva prije otvaranja privitaka te upozoravati korisnika pri preuzimanju datoteka i programa s interneta. Antivirusni programi, zavisno o izvedbi, rade na dva načina. Prvi način je skeniranje ulaza u računalo i samog računala kako bi se otkrilo postojanje „otisaka" zloćud-

nih programa, kako je prethodno opisano. Preduvjet za to je da je antivirusna tvrtka identificirala neki „otisak" kao zloćudni program, zbog čega je bitno periodički ažurirati bazu zloćudnih programa u okviru antivirusnog alata. Međutim, na ovaj se način neće moći otkriti nove prijetnje koje nisu identificirane kao zloćudni programi. Zato je drugi način rada naprednijih alata nadzor sustava i programa koji se izvode kako bi se utvrdili rizični obrasci. Tako će, primjerice, biti sumnjiv program koji pristupa resursima koji mu zapravo ne trebaju, podatcima drugih programa ili aplikacija, koji otvara mrežne konekcije iz nejasnih razloga i slično. Sustavi koji imaju ovakvu funkcionalnost nadzora računala na toj razini ubrajaju se u domenu sustava za otkrivanje uljeza (engl. intrusion detection system). Eventualna mana takvih sustava jest da neće moći uvijek prepoznati je li neki program doista prijetnja, ali i da će nekada legitimne programe označiti prijetnjom. Kod takvih programa često se daje obavijest korisniku koji sam treba odlučiti što napraviti, što često nije dobra praksa jer korisnici u pravilu nemaju dovoljno tehničkih znanja da bi mogli razumjeti što podatci koje im takav sustav nudi zapravo znače.

Gledano s motrišta krajnjeg korisnika koji želi koristiti sve dostupne usluge, potrebno je reći kako rizik uvijek postoji i nije moguće imati potpuno siguran sustav. Ova tvrdnja posebice stoji zbog spomenutih *zero-day* ranjivosti koje svaki sustav ima, no još nisu otkrivene. Ukoliko ih napadač otkrije prije proizvođača operacijskoga sustava ili pojedinih aplikacija, iskorištavanje ranjivosti je vrlo izgledno, često bez obzira na prisutnu zaštitu u smislu antivirusnih alata.

S obzirom da je najčešći vektor napada još uvijek *phishing* s nekom vrstom društvenog inženjeringa, korisnici bi trebali biti izrazito sumnjičavi kada dobivaju poruke sumnjivog sadržaja i uvijek provjeriti istinitost tih poruka prije nego li postupe po uputama i odaju vlastitu lozinku ili instaliraju potencijalno zloćudni program. Što se tiče mrežnih prijetnji, potrebno je redovito i što prije ažurirati nove zakrpe, odnosno nadogradnje operacijskog sustava i aplikacija koje koriste jer je cilj zakrpa, između ostalog, doraditi eventualno pronađene sigurnosne propuste. Tako će se onemogućiti iskorištavanje pronađenih ranjivosti čime se značajno može spriječiti djelovanje zloćudnih programa kao što su crvi koji se šire mrežom.

Konačno, korisnici ne bi smjeli nasjedati na ponude besplatnih sadržaja, programa i medija, koje mogu preuzeti s ilegalnih servisa kao što je *torrent* ili s ilegalnih mrežnih sjedišta koja nude besplatne inačice programa i alata.

4.5. LITERATURA

Bortnik, S. (6. studenog 2013). *Five interesting facts about the Morris worm*. Preuzeto s https://www.welivesecurity.com/2013/11/06/five-interesting-facts-about-the-morris-worm-for-its-25th-anniversary/, 15.8.2018.

Ducklin, P. (16. rujna 2011). *Memories of the Nimda virus*. Preuzeto s https://nakedsecurity.sophos.com/2011/09/16/memories-of-the-nimda-virus/, 15.8.2018.

Holloway, M. (16. srpnja 2015). *Stuxnet Worm Attack on Iranian Nuclear Facilities*. Preuzeto s http://large.stanford.edu/courses/2015/ph241/holloway1/, 15.8.2018.

Kaspersky. (2018). *Kaspersky web site online*. Preuzeto s https://www.kaspersky.com, 15.8.2018.

Keshet L. (25. siječnja 2017). *Anatomy of an hVNC Attack*. Preuzeto s https://securityintelligence.com/anatomy-of-an-hvnc-attack/, 15.8.2018.

KnowBe4: AIDS Trojan or PC Cyborg Ransomware. (2018). *KnowBe4's Ransomware Knowledgebase online.* Preuzeto s https://www.knowbe4.com/aids-trojan, 15.8.2018.

Palmer, D. (11. svibnja 2018). *WannaCry ransomware crisis, one year on: Are we ready for the next global cyber attack*? Preuzeto s https://www.zdnet.com/article/wannacry-ransomware-crisis-one-year-on-are-we-ready-for-the-next-global-cyber-attack/, 15.8.2018.

Peikari, C., Fogie, S., Read, J., i Hettel, D. (2004). *Summer Brings Mosquito-Borne Malware*. Preuzeto s http://www.informit.com/articles/article.aspx?p=327994, 15.8.2018.

SETI@home. (2018). *SETI@home Project online*. Preuzeto s https://setiathome.berkeley.edu/, 15.8.2018.

Tequila. (2018). *F-Secure Corporation's Threat description online*. Preuzeto s https://www.f-secure.com/v-descs/tequila.shtml, 15.8.2018.

The Most Famous Virus History: Melissa, A. (2013). Panda Security's mediacenter online. Preuzeto s https://www.pandasecurity.com/mediacenter/malware/most-famous-virus-history-melissa/, 15.8.2018.

The Michelangelo Virus, 25 Years Later. (2017). *Trend Micro Inc. news online*. Preuzeto s https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-michelangelo-virus-25-years-later, 15.8.2018.

Virus Creeper. (b.d.). U: The Virus Encyclopedia. Preuzeto s http://virus.wikidot.com/creeper, 11.8.2018.

Virus Jerusalem. (2017). *Malware Wiki*. Preuzeto s http://malware.wikia.com/wiki/Jerusalem, 13.8.2018.

Virus NYB. (2000). *Symantec's Security centre online*. Preuzeto s https://www.symantec.com/security-center/writeup/2000-121513-2227-99, 15.8.2018.

What is CryptoLocker? (b.d.). *Avast Software online*. Preuzeto s https://www.avast.com/c-cryptolocker, 15.8.2018.

What is the difference between viruses, worms, and Trojans? (2016). *Symantec's Technical Support online*. Preuzeto s https://support.symantec.com/en_US/article.TECH98539.html, 15.8.2018.

Zeus Virus. (2018). *Kaspersky Lab's threats online*. Preuzeto s https://usa.kaspersky.com/resource-center/threats/zeus-virus, 15.8.2018.

Kaspersky: Cryptolocker Virus Definition (2018). Preuzeto s https://usa.kaspersky.com/resource-center/definitions/cryptolocker, 15.8.2018.

izv. prof. dr. sc. Krešimir Nenadić
Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek

5. MREŽNA SIGURNOST

Sažetak

Poglavlje daje pregled mrežne sigurnosti kao i preporuke korisnicima kako održati sigurnost, prvo svog uređaja, a zatim i cijele mreže, odnosno informacijskog sustava. Definirana je sigurnosna politika koja propisuje pravila i procedure koje svi korisnici mreže trebaju provoditi. U nastavku su navedeni tipovi mrežne sigurnosti i za većinu tipova su navedene preporuke kako izbjeći neželjene događaje s ciljem održavanja određene razine sigurnosti mreže.

5.1. UVOD

Prema definiciji koju navodi CISCO (2018), vodeća kompanija mrežnih tehnologija, mrežnu sigurnost predstavlja skup aktivnosti čiji je cilj zaštititi iskoristivost i cjelovitost računalne mreže i podataka. Za provođenje zaštite mreže potrebno je uključiti i sklopovske (engl. *hardware*) i programske (engl. *software*) tehnologije. Kako bi mrežna sigurnost bila na poželjnom nivou, potrebno je kvalitetno upravljati pristupu mreži i mrežnim resursima. Pristup mreži podrazumijeva komunikaciju s uređajima u ciljanoj mreži, a mrežni resursi predstavljaju usluge koje se pružaju u ciljanoj mreži. Usluge mogu biti pristup datotečnom poslužitelju, pristup mrežnom poslužitelju, korištenje usluge e-pošte i druge usluge. Same aktivnosti mrežne sigurnosti imaju cilj detektirati različite prijetnje unutar i izvan mreže i spriječiti širenje ili ulazak prijetnji u mrežu.

Mrežna sigurnost se provodi kroz više slojeva i na različitim dijelovima mreže. Neke od aktivnosti vezane za sigurnost provode se na samom rubu mreže (engl. *gateway*), ali i na gotovo svim uređajima unutar mreže. Na svakom sloju mrežne sigurnosti mogu se primijeniti sigurnosne politike i kontrola prometa, odnosno podataka.

Prema kompaniji Palo Alto Networks (2018), jednoj od vodećih u području cybersigurnosti, sigurnosnu politiku predstavlja niz pravila i procedura za sve osobe koje pristupaju i koriste imovinu i resurse u vlasništvu organizacije. Sigurnosna politika se definira prema načinu odnosa korisnika mreže prema sigurnosti mreže. Stoga je sigurnosna politika jedinstveni dokument svake organizacije. Cilj sigurnosne politike je očuvanje povjerljivosti, cjelovitosti i dostupnosti sustava, odnosno mreže koju koriste članovi organizacije u čijem je vlasništvu mreža. Budući da se ponašanje zaposlenika tijekom vremena mijenja, konstantno je potrebno prilagođavati i sigurnosnu politiku. To je, dakle, dokument podložan stalnim promjenama u smislu poboljšavanja ukupne sigurnosti mreže.

Pitanje sigurnosti mreže ne čini samo jedan element nego sprega većeg broja elemenata. Postoje dvije krajnosti po pitanju sigurnosti računalne mreže - mreža može biti potpuno sigurna (zatvorena) ili potpuno otvorena s potpunim pristupom. Ni jedna navedena krajnost nije preporučljiva. Ako je mreža potpuno sigurna i zatvorena, korisnici neće imati pristup dijelovima potrebnih resursa (pristup datotečnom poslužitelju, intranetu ili nekoj drugoj usluzi). U slučaju druge krajnosti, kada je mreža potpuno otvorena, zlonamjerni napadač bez problema može pristupiti mrežnim resursima i „narediti" drugom računalu da napravi nešto što nije dopušteno.

Svaka organizacija mora procijeniti kako i koliko će zaštititi svoju mrežu. Dio zaštite mreže je i donošenje određenih pravila ponašanja korisnika mreže, politike sigurnosti u obliku zahtjeva i preporuka čime se definiraju sigurnosne mjere i rizici.

Sigurnosne mjere i politiku postavlja uprava organizacije na prijedlog nadležne službe u organizaciji. O provedbi mrežne zaštite brine se mrežni administrator. Zaštita mreže provodi se tako da se sprječava neovlašteni pristup mrežnim resursima. Resursima koji imaju ograničen pristup trebali bi pristupati samo za to ovlaštene osobe ili uređaji. Uz zaštitu potreban je stalni nadzor rada mreže (mrežnih uređaja) i procjena učinkovitosti.

5.2. KONTROLA PRISTUPA MREŽI

Kada se promatra računalna mreža u vlasništvu neke organizacije, pristup toj mreži je ograničen na ovlaštene osobe, najčešće zaposlenike te organizacije. U ovoj skupini se ovlaštene osobe mogu kategorizirati u više skupina s različitim pravima pristupa mrežnim resursima i uslugama. Sustav može napraviti identifikaciju samog korisnika ili uređaja kojim se pristupa mreži ili usluzi. Identifikacija je prvi korak vezan za mrežnu sigurnost.

Korisnik se identificira svojim korisničkim imenom (engl. *username*) pri pristupu mrežnim resursima ili uslugama. Samo ovlašteni korisnici mogu pristupiti mreži, dijelovima mreže ili određenim uslugama. Identifikacija korisnika obavlja se provjerom postojanja korisničkog imena s popisom ovlaštenih osoba u bazi podataka na nekom od poslužitelja. Ako se korisničko ime nalazi na popisu u bazi podataka, korisniku će se dopustiti pristup ovisno o njegovim ovlastima koje su definirane sigurnosnom politikom.

Uređaj se isto tako može identificirati prilikom pristupa mreži. Na najnižem sloju modela mreže prema OSI (engl. *Open Systems Interconnection*) mrežnom modelu (ISO standard, 2018), pristup mreži se može ograničiti kontrolom fizičkog pristupa priključcima za mrežnu komunikaciju. Slojevi OSI mrežnog modela prikazani su na Slici 1. Zaposlenici organizacije mogu pristupati mreži na različite načine. Obično u svom uredu zaposlenici imaju fizički mrežni priključak (RJ45) na koji uređaj spajaju mrežnim kablom. Nakon što zadnji zaposlenik napusti ured, prostorija bi se trebala zaključati kako neovlaštene osobe ne bi imale fizički pristup mrežnim priključcima. Budući da većina zaposlenika nema pristup mrežnoj opremi (usmjerivači, preklopnici, poslužitelji), gledište koje se tiče zaštite takvih uređaja neće biti obrađeno u ovom poglavlju. O sigurnosti navedenih uređaja brinu se mrežni administratori koji su educirani i stručni obav-

ljati zaštitu mreže i mrežnih uređaja. Drugi način pristupa mreži je preko bežične mreže (engl. *WiFi*) za koji nije potreban fizički priključak pa se identifikacija uređaja obavlja drugačije.

Slika 1.
Slojevi OSI mrežnog modela

Bez obzira na način pristupa mreži, fizički pristup mrežnim kablom ili putem bežične konekcije, identifikacija samih uređaja koji pristupaju mreži i njenim resursima obavlja se u nekoliko slojeva OSI mrežnog modela. Na drugom sloju OSI modela (sloj podatkovne veze) identifikacija uređaja obavlja se pomoću fizičke adrese uređaja (engl. *Media Access Controll* MAC address). Fizička adresa uređaja je jedinstvena, zapisana u samom uređaju i u pravilu se ne može mijenjati. Primjer fizičke adrese nekog uređaja je: **E89A8FC7C8BD**. Kontrola pristupa mreži pomoću fizičke adrese uređaja izvršava se na preklopniku koji prati promet podataka i uspoređuje fizičke adrese unutar podataka s onima u svojim postavkama. Na taj način može dopustiti ili zabraniti promet ovisno o postavkama koje je podesio administrator mreže. Filtriranje prometa usporedbom fizičkih adresa uređaja ne ovisi o načinu spajanja na mrežu (kabel ili bežični pristup).

Na mrežnom sloju OSI modela identifikacija uređaja se obavlja na osnovu mrežne ili IP adrese. Mrežna adresa je isto tako jedinstvena oznaka uređaja. Ako je mrežna adresa javna, mora biti jedinstvena za cijeli svijet (internet). U slu-

ju korištenja privatnih mrežnih adresa, uređaj treba imati jedinstvenu mrežnu adresu unutar te privatne mreže. Kao što preklopnik može obavljati kontrolu (filtriranje) prometa na osnovu fizičke adrese, tako usmjerivač obavlja istu funkciju na osnovu mrežnih adresa. Ovisno o postavkama usmjerivača, određeni promet se može propustiti ili zabraniti prije ulaska u mrežu ili napuštanja mreže. Osim po mrežnim adresama, usmjerivač može filtrirati promet i po tipu komunikacije, odnosno protokolu koji se koristi prilikom komunikacije.

Kao primjer može se navesti pokušaj pristupanja uslugama neke ustanove kojima se može pristupiti samo s uređaja koji su unutar mreže te ustanove. Ako, na primjer, korisnik čiji uređaj ima IP adresu 145.50.22.88 pokuša pristupiti uslugama na poslužitelju s IP adresom 131.24.99.1, pristup će mu biti odbijen jer korisnikov uređaj nema IP adresu u istoj mreži kao poslužitelj. Provjerom IP adresa može se ograničiti ili potpuno onemogućiti pristup uređajima koji su u rizičnim skupinama ili zemljama na osnovu IP adrese pristupnog uređaja. Ograničenja, odnosno dozvola ili zabrana prometa na osnovu IP adrese se mogu definirati za oba smjera komunikacije. Tako se, na primjer, zaposlenicima neke ustanove može zabraniti pristup nekoj usluzi koju ne pruža ta ustanova. Najčešće poslodavci brane svojim zaposlenicima posjećivanje društvenih mreža za vrijeme radnog vremena ili sa službenih računala. U takvom slučaju je administrator sustava upisao IP adresu poslužitelja društvene mreže u pristupnu listu i toj IP adresi je zabranjen pristup s uređaja koji se nalaze u mreži ustanove. Na sličan način, ali provjerom tipa komunikacije po broju komunikacijskog porta, može se dopustiti ili zabraniti pristup određenim uslugama prema vrsti usluge, odnosno prema vrsti prometa.

Drugi dio kontrole pristupa mreži je autentikacija korisnika. Nakon identifikacije korisničkog imena potrebno je utvrditi je li to stvarno korisnik koji se mreži ili mrežnoj usluzi predstavlja. Autentikacija se obavlja provjerom zaporke koju korisnik upisuje s onom u bazi podataka koja je postavljena prilikom registracije korisnika. Korisnici mogu imati pravo promjene zaporke na neku novu vrijednost. Kvalitetu zaporke, pa time i sigurnost koja se ostvaruje autentikacijom, određuje sigurnosna politika organizacije. Više o kvaliteti zaporke može se pronaći u radovima autora Šolić, Očevčić i Blažević (2015) te u Šolić, Kralik, Ilakovac i Nenadić (2014).

Nakon uspješne identifikacije i autentikacije uređaja ili korisnika, može se pristupiti određenim mrežnim resursima. Kojim mrežnim resursima i uslugama može pristupiti određeni korisnik određuje se sigurnosnom politikom.

5.3. PROGRAMI ZA ZAŠTITU PROTIV VIRUSA I ZLOĆUDNIH PROGRAMA

Svaki korisnik uređaja kojim se spaja na bilo kakvu mrežu treba se zaštititi od raznih vrsta zlođudnih programa. Vrste zlođudnih programa objašnjene su poglavlju o *Osobnoj sigurnost i zlođudnim programima na internetu* ove knjige. Preporuka svakom korisniku je instalacija programa (aplikacija) koja će uređaj štititi od napada zlođudnih programa. Postoje besplatni alati koji na zadovoljavajući način mogu zaštititi uređaj. Korisnik uređaja se treba pobrinuti za redovito osvježavanje same aplikacije novim nadogradnjama, kao i preuzimanjem najnovijeg popisa zlođudnih programa kako bi se učinkovitozaštitio od njih.

Kako svaki korisnik treba zaštititi svoj uređaj odgovarajućom aplikacijom protiv zlođudnih programa, tako administrator treba zaštititi poslužitelje od istih prijetnji. Svaki uređaj za svoj normalni rad treba operacijski sustav koji se brine o normalnom funkcioniranju uređaja. Sam operacijski sustav obično nema funkcionalnost koja štiti uređaj od zlođudnih programa pa je takve aplikacije potrebno naknadno instalirati. Aplikacije za zaštitu od zlođudnih programa se razlikuju prema vrsti operacijskog sustava na koji se instaliraju. Osim vrste operacijskog sustava razlikuju se i aplikacije za zaštitu poslužitelja od onih za zaštitu krajnjeg korisnika mrežnih usluga. Postoje programska rješenja koja objedinjuju više funkcionalnosti u zaštiti uređaja, ali se korisnik može odlučiti i na usko specijalizirane aplikacije koje nude zaštitu od samo jedne vrste zlođudnih programa. Ako je uređaj koji treba zaštititi poslužitelj, administrator u dogovoru s upravom organizacije i sigurnosnom politikom treba odlučiti koji aplikaciju ili aplikacije za zaštitu će postaviti na poslužitelj. Odabir ovisi i o financijskom čimbeniku jer su aplikacije za poslužitelje uglavnom komercijalne i cijena im nije niska. Za klijentske uređaje može se odabrati i neko od besplatnih rješenja koje se može preuzeti s interneta ili više različitih aplikacija. Pri instalaciji aplikacija za zaštitu uređaja ne treba pretjerivati u njihovom broju jer neke od aplikacija mogu usporiti rad uređaja ili, u još gorem slučaju, neke aplikacije ne mogu raditi u isto vrijeme s drugim aplikacijama.

Postoji mogućnost zadavanja obvezne aplikacije za zaštitu ako je tako definirano sigurnosnom politikom i ako se takva aplikacija kupi. Čest slučaj je da vlasnik aplikacije prodaje obje vrste aplikacije - za poslužitelje i za klijentska računala. U tom slučaju korisnik nema mogućnost odabira aplikacije, već bi trebao koristiti onu koja je definirana sigurnosnom politikom.

5.4. ZAŠTITA APLIKACIJA

Bilo koja aplikacija, odnosno programsko rješenje, koje organizacija koristi u svom radu treba biti zaštićena. Zaštita aplikacija obuhvaća mjere koje su poduzete kako bi se ostvarila ili povećala sigurnost. Mjere koje se mogu poduzeti su traženje, popravljanje i sprječavanje ranjivosti same aplikacije. Od dijelova životnog ciklusa aplikacije ovdje nas zanima postavljanje, nadogradnja i održavanje aplikacije.

Prilikom izrade aplikacije mogu se pojaviti različiti propusti koji napadaču omogućuju iniciranje različitih vrta napada na aplikaciju, a preko aplikacije i na cijeli sustav, odnosno mrežu. Propusti mogu biti uzrokovani i greškama u prevoditelju programskog kôda.

Bez obzira na vrstu propusta, gdje i kada je nastao, mogu se otkloniti programskim nadogradnjama. Aplikacije obično imaju mogućnost automatskog preuzimanja nadogradnji i njihovihinstalacija. U slučaju kada ne postoji automatsko preuzimanje i instalacija nadogradnji, iste je potrebno obaviti ručno. Nadogradnja aplikacije sigurnosnom zakrpom se onda obavlja preuzimanjem samo zakrpe ili preuzimanjem nove inačice cijele aplikacije koja sadrži i samu zakrpu.

5.5. ANALIZA PONAŠANJA

Kako bi se detektiralo abnormalno ponašanje uređaja ili korisnika, potrebno je znati ili definirati kako izgleda normalno ponašanje ili funkcioniranje uređaja ili korisnika. Kao što uređaji svojim radom u mrežnom okruženju mogu biti izvor smetnji ili prijetnji, tako i korisnici koji ih koriste svojim ponašanjem tijekom rada na uređaju mogu biti izvor prijetnji. Postoje programski alati koji mogu detektirati ponašanje ili funkcionalnosti koje odstupaju od normalnog ili definiranog sigurnosnom politikom. Praćenje ponašanja sustava, mreže, uređaja i korisnika je kontinuirani proces čiji je cilj održavanje sigurnosti sustava, odnosno cijele mreže.

Korisnik svojim radom na uređaju može narušiti sigurnost mreže te tako postaje izvor prijetnje mrežnoj sigurnosti. U privitku poruke epošte korisnik može dobiti datoteku čijim se pokretanjem izvršava neki maliciozni program koji se može proširiti na druge uređaje unutar mreže. Još jedan oblik narušavanja sigurnosti je priključivanje tuđih neprovjerenih memorijskih štapića na uređaj koji je spojen na mrežu. Čest oblik narušavanja sigurnosti na strani korisnika je slanje svojih pristupnih podataka osobama koje zatraže te podatke. Važno je naglasiti

da administrator sustava nikada neće tražiti pristupne podatke od bilo kojeg korisnika tog sustava.

Više o sigurnosti sustava i načinima procjene može se pronaći u radovima autora Šolić, Očevčić i Golub (2014), Očevčić, Nenadić, Šolić i Keser (2017) i Velki, Šolić i Nenadić (2015). O sigurnosti, prijetnjama i rješenjima vezanih za društvene mreže može se pronaći u radovima autora Rathore i drugi (2017) i Tayouri (2015).

5.6. GUBITAK PODATAKA

Prijetnju sigurnosti sustava, odnosno mreže može predstavljati gubitak podataka. Podatci s bilo koje vrste poslužitelja napadom se mogu obrisati, odnosno trajno uništiti. Postoje slučajevi napada na mreže, konkretno na poslužitelje čiji je cilj bio preuzimanje, odnosno kopiranje podataka o računima, odnosno o brojevima kreditnih kartica korisnika usluga nekog mrežnog sustava. Jedan od možda najpoznatijih napada je onaj na Sony gdje su napadači prikupili podatke kreditnih kartica korisnika Sony PlayStation uređaja. Detalji o napadu se mogu pogledati na stranici Eurogamera: https://www.eurogamer.net/articles/2016-04-26-sony-admitted-the-great-psn-hack-five-years-ago-today (2016).

Teži oblik napada na podatke je brisanje podataka s poslužitelja ili klijentskog računala. Zaštita od ovakve vrste napada gdje se podatci brišu, odnosno uništavaju, je kreiranje kopije podataka na nekom vanjskom uređaju za pohranu podataka ili korištenje usluge na internetu za spremanje podataka. Podatci se mogu duplicirati na nekoj od besplatnih usluga koje nude pohranu podataka u obliku dokumenata ili datoteka.

O zaštiti podataka na poslužiteljima se brine mrežni administrator. Svaki korisnik se treba pobrinuti o održavanju sigurnosne kopije podataka sa svakog svog uređaja. Sinkronizaciju podataka na uređaju i sigurnosne kopije treba obavljati periodički, ovisno o korisnikovim potrebama.

Neke usluge na internetu nude mogućnost sinkronizacije podataka na uređaju i podataka na njihovom poslužitelju. Korisnik može mijenjati podatke unutar datoteka na svom uređaju neovisno ima li poveznicu na internet ili nema, a sinkronizacija se obavlja kada uređaj ostvari povezivanje na internet.

Od gubitka podataka najsigurnije rješenje je održavanje jedne ili više kopija, barem najbitnijih podataka.

U zadnje vrijeme se pojavio način napada gdje zloćudni program (engl. *ransomware*) kriptira korisničke podatke na uređaju i traži od korisnika plaćanje

određene svote novca na račun kako bi dobio ključ za otključavanje kriptiranih podataka. I za ovakav slučaj gubitka podataka najjednostavniji način povrata „*izgubljenih*“ podataka je iz sigurnosne kopije.

5.7. SIGURNOST E-POŠTE

E-pošta je jedan od najvećih izvora prijetnji sigurnosti mreže. U zadnje smo vrijeme svjedoci personaliziranih napada, ili barem pokušaja, gdje napadač šalje personaliziranu poruku potencijalnoj žrtvi. Poruka sadrži informacije koje su rezultat socijalnog inženjeringa i taktike „*pecanja*“ (engl. *phishing*) kojima korisnika nagovaraju na razne štetne akcije. U privitku poruke može biti dio zloćudnog kôda koji se može izvršiti i samim otvaranjem poruke, bez korisničkog otvaranja privitka. Šteta koju može nanijeti zloćudni program ili kôd u privitku ne mora biti ograničena samo na korisnikov uređaj, već se zloćudni kôd može mrežom proširiti i na druge uređaje posredstvom poslužitelja.

Preporuka korisnicima je ne otvarati poruke nepoznatih pošiljatelja, a svakako ne otvarati privitke u takvim porukama. Postoje aplikacije koje mogu spriječiti preuzimanje zloćudnog koda iz eporuke, ali se taj problem može riješiti i na poslužitelju. Dobra zaštita na e-pošti poslužitelju može onemogućiti primanje poruka sa zloćudnim sadržajima.

Još jedan oblik napada na e-poštu korisnika je primanje neželjene pošte (engl. *spam*). Poruka koja kao odredište ima veći broj korisnika e-pošte može biti okarakterizirana kao neželjena poruka. O filtriranju ovakvih poruka na poslužitelju brine se administrator, ali i svaki korisnik može u aplikaciji koju koristi za čitanje e-pošte podesiti filter za kontrolu neželjenih poruka.

5.8. VATROZID

Vatrozid (engl. *firewall*) je usluga u obliku sklopovskog i/ili programskog rješenja, koja predstavlja prepreku koja se nalazi između poznate i pouzdane mreže i nepoznate nepouzdane mreže koju može predstavljati internet. Vatrozid koristi skup definiranih pravila koja dopuštaju ili zabranjuju promet u oba smjera - u mrežu ili iz mreže.

Slijedi primjer konfiguracije pristupne liste (engl. *access list*) na usmjerivaču s objašnjenjima. Korisnik koji konfigurira pristupnu listu treba imati odgovarajuće administratorske ovlasti za uređaj na kojemu se vrši konfiguracija.

Primjer 1.
Naredbe za postavljanje pristupnih lista na usmjerivaču

Naredba ili akcija	Svrha
`Device(config)# ip access-list standard AccessList1`	Definira se standardna IP pristupna lista korištenjem imena (AccessList1)
`Device(config-std-nacl)# deny 172.16.0.0 0.0.255.255`	Svim uređajima koji pripadaju mreži s IP adresom 172.16.0.0 zabranjuje se (engl. *deny*) dolazni promet prema lokalnoj mreži u vlasništvu ustanove u kojoj se nalazi usmjerivač koji se konfigurira.
`Device(config-std-nacl)# permit 172.18.5.22 0.0.0.0`	Uređaju s IP adresom 172.18.5.22 se dopušta (engl. *permit*) prolazak kroz pristupnu listu, odnosno dopušta se dolazni promet.
`Device(config-ext-nacl)# deny ip 172.18.0.0 0.0.255.255 host 172.16.40.10`	Svim uređajima koji pripadaju mreži s IP adresom 172.18.0.0 zabranjuje se sav promet prema uređaju s IP adresom 172.16.40.10

Vatrozid može biti postavljen na pojedini poslužitelj s ciljem filtriranja mrežnog prometa. Na taj način se može smanjiti količina podataka koja putuje pojedinim dijelom mreže. Osim na poslužiteljima, vatrozid može biti postavljen, odnosno konfiguriran, na usmjerivaču koji predstavlja ulaz/izlaz mreže (engl. *gateway*). Isto tako vatrozid je moguće konfigurirati na klijentskim uređajima kao dio operacijskog sustava ili kao zasebnu aplikaciju. Korisnik treba voditi računa da ako poslužitelji i/ili *gateway* imaju podešen vatrozid, uređaj bi trebao imati vatrozid istog proizvođača kako ne bi došlo do nemogućnosti mrežne komunikacije.

5.9. SUSTAVI ZA SPRJEČAVANJE UPADA

Sustav za sprječavanje upada u mrežu (engl. *Intrusion Prevention Systems* IPS) nadzire mrežni promet s ciljem aktivnog blokiranja napada na mrežnu sigurnost. IPS sustavi su veliki sustavi koji imaju mogućnost pamćenja, odnosno bilježenja prijetnji, a neki imaju i mogućnost strojnog učenja s ciljem što veće učinkovitosti sprječavanja neželjenih napada. Osim što mogu blokirati zloćudne aktivnosti, IPS sustavi mogu pratiti progresiju sumnjivih datoteka i zloćudnih programa i kôdova kroz mrežu kako bi spriječili izbijanje i širenje zaraženog, odnosno zloćudnog kôda.

5.10. MOBILNI UREĐAJI

Svjedoci smo naglog razvoja i širenja popularnosti mobilnih uređaja, prvenstveno pametnih telefona i tableta, pa su i takvi uređaji postali cilj napada. U slijedeće 3 godine 90% organizacija u IT sektoru će podržavati korporacijske aplikacije na mobilnim uređajima (CISCO, 2018). Samim time mobilni uređaji postaju zanimljivi napadačima pa je i njih potrebno nekako zaštititi. Na tržištu već postoje aplikacije za zaštitu, kako samih uređaja, tako i podataka na njima.

I ovdje vrijedi preporuka o izradi sigurnosne kopije osjetljivih podataka. Na mobilnim uređajima osjetljivi podatci mogu biti i kontakti u imeniku uređaja, poruke, pa i datoteke. Mobilni uređaji uglavnom uz operacijski sustav imaju i potrebne funkcionalnosti za sinkronizaciju podataka na uređaju s onima sigurnosne kopije.

Sustavi plaćanja mobilnim uređajem s poslužiteljem komuniciraju putem sigurnih protokola pri čemu se razmjenjuju kriptirani podatci. Svi korisnikovi podatci koji se šalju poslužitelju se kriptiraju na mobilnom uređaju te se šalju poslužitelju u kriptiranom obliku. Na strani poslužitelja kriptirani podatci se dekriptiraju kako bi se utvrdio identitet korisnika.

Više o sigurnosti korištenja mobilnih uređaja za različite oblike komunikacije može se pogledati u radu autora La Polla, Martinelli i Sgandurra (2012).

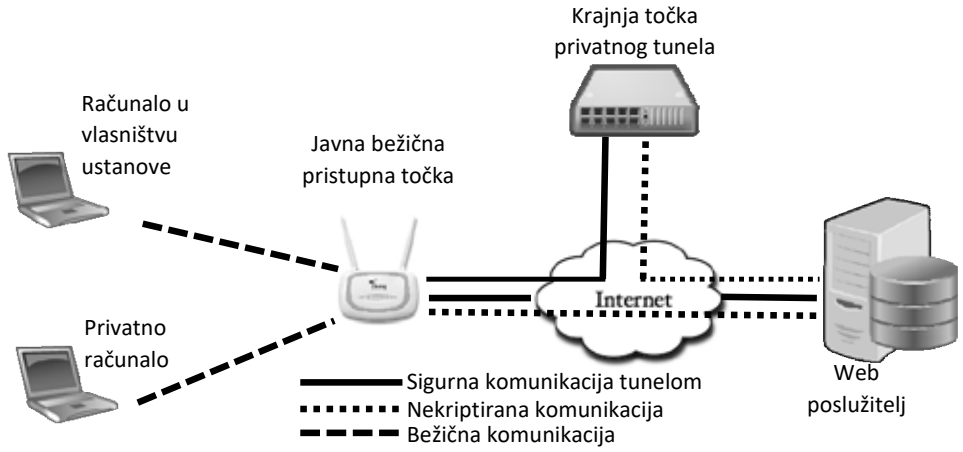
5.11. SEGMENTACIJA MREŽE

Programski definirana segmentacija mreže, odnosno podjela na manje logičke cjeline, pruža mogućnost klasificiranja mrežnog prometa te se tako lakše provodi sigurnosna politika. U idealnom slučaju klasifikacija se temelji na identifikaciji uređaja koji se spaja na mrežu ili je već spojen neovisno o mrežnoj adresi. Uređaju, odnosno korisniku koji koristi uređaj, mogu se dodijeliti prava pristupa pojedinim mrežnim resursima temeljem uloge koju obavlja u organizaciji, lokacije gdje se korisnik nalazi ili ovisno o nekom drugom kriteriju. Na taj se način odgovarajućim korisnicima dodjeljuju odgovarajuća prava pristupa, a sumnjivim korisnicima, odnosno njihovim uređajima se može zabraniti pristup i restriktivno reagirati na određeni način ovisno o sigurnosnoj politici.

5.12. VIRTUALNA PRIVATNA MREŽA

Svrha virtualne privatne mreže je omogućiti ovlaštenim korisnicima koji su fizički izdvojeni od svoje mreže na nekoj drugoj geografskoj lokaciji sigurnu komunikaciju s mrežom. Takva komunikacija se obično kriptira, a za povezivanje dvije geografski udaljene točke koristi se internet. Tako se udaljenom korisniku čini kao da se nalazi unutar svoje mreže i može koristiti sve resurse kao da se fizički nalazi unutar mreže. Primjer virtualne privatne mreže može se vidjeti na Slici 2.

Postupak kriptiranja je pretvorba informacije (na primjeru običnog teksta) u oblik koji mogu protumačiti samo autorizirane osobe koje znaju kako se kriptirani tekst ponovno pretvara u izvorni oblik postupkom dekriptiranja. Na taj način se osjetljive informacije mogu zaštititi tako da ih ne može protumačiti bilo tko.



Slika 2.
Prikaz komunikacije preko VPN mreže

5.13. LITERATURA

35.100 OSI model. (1994). *International Organization for Standardization's store online.* Preuzeto s https://www.iso.org/ics/35.100/x/, 12.9.2018.

Eurogamer. (2016). Five years ago today, Sony admitted the great PSN hack. Preuzeto s https://www.eurogamer.net/articles/2016-04-26-sony-admitted-the-great-psn-hack-five- years-ago-today, 12.9.2018.

Gregory, B. W., Eric, A. F. i Udo, W. P. (2017). *Computer System and Network Security*. Boca Raton, USA: CRC Press

La Polla, M., Martinelli, F. i Sgandurra, D. A Survey on Security for Mobile Devices. *IEEE: IEEE Communications Surveys & Tutorials, Vol. 15, 446-471*

Odom, W. (2016). CCNA Routing and Switching 200-125 Official Cert Guide Library. USA: Cisco Press

Očevčić, H., Nenadić, K., Šolić, K. i Keser, T. (2017). The Impact of Information System Risk Management on the Frequency and Intensity of Security Incidents. *International journal of electrical and computer engineering systems, 8,* 41-46.

Rathore S., Sharma, K. P., Loia V., Jeong Y.-S. i Park J. H. (2017). Social network security: Issues, challenges, threats, and solutions. *Elsevier: Information Sciences, Vol. 421, 43-69*

Šolić, K., Kralik, K., Ilakovac, V., i Nenadić, K. (2014). Lakovjernost ili preposlušno praćenje predavaćevih instrukcija (otkrivanje zaporke). *Medix: specijalizirani medicinski dvomjesečnik, 109/110*, 239-242.

Šolić, K., Očevčić, H., i Blažević, D. (2015). Survey on Password Quality and Confidentiality. *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije, 56,* 69-75.

Šolić, K., Očevčić, H., i Golub, M. (2014). The information systems' security level assessment model based on an ontology and evidential reasoning approach. *Computers & security, 55,* 100-112.

Tayouri, D. (2015). The Human Factor in the Social Media Security - Combining Education and Technology to Reduce Social Engineering Risks and Damages. *Elsevier: Procedia Manufacturing, Vol. 3, 1069-1100*

Velki, T., Šolić, K. i Nenadić, K. (2015). Razvoj i validacija Upitnika znanja i rizičnog ponašanja korisnika informacijskog sustava (UZPK). *Psihologijske teme, 24,* 401-424.

What is an It security policy? (b.d.). *PaloAlto Networks's CyberPedia online*. Preuzeto s https://www.paloaltonetworks.com/cyberpedia/what-is-an-it-security-policy, 12.9.2018.

What is network security? (b.d.). *CISCO's Security products online*. Preuzeto s https://www.cisco.com/c/en/us/products/security/what-is-network-security.html, 12.9.2018.

Ivan Horvat
OTIS d.o.o, Osijek

doc. dr. sc. Krešimir Šolić
Medicinski fakultet Osijek

6. OSNOVE KRIPTOGRAFIJE

Sažetak

Prosječan korisnik informacijskokomunikacijskih sustava danas učestalo koristi kriptografiju, a da možda toga nije nisvjestan. Od kriptiranih zaporki za raznorazne sustave do digitalnih ceritifikata za pristupanje internetskog bankarstvu ili sustavu egrađani. Čak je i običan telefonski razgovor putem analogne linije vrsta kripto sustava, budući da koristi frekvencijsku modulaciju ljudskoga glasa, ali s javno poznatim simetričnim ključem.

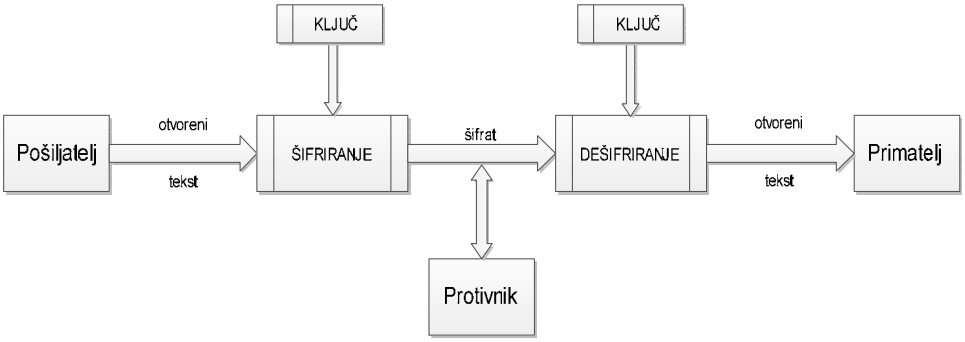
Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje tajnih poruka u obliku koji će moći pročitati samo primatelj kojemu je i namijenjena, a počela se upotrebljavati još u staroj Grčkoj, gdje su Spartanci u 5. stoljeću prije Krista koristili napravu za šifriranje nazvanu skital.

U ovome poglavlju opisan je povjesni razvoj kriptografije, opisani su osnovni načini i mehanizmi kriptiranja i dekriptiranja podataka s jednostavnim primjerima, te je kratko opisana kriptografija u današnjoj praktičnoj upotrebi.

Prosječan korisnik, radi osobne zaštite te zaštite raznih informacijsko-komunikacijskih sustava koje koristi, treba biti svjestan kako je izrazito važno čuvati tajnost svojih pristupnih podataka navedenim sustavima te kako je on odgovoran za sve što se pod njegovim imenom na tim sustavima pojavljuje i mijenja. Kriptiranje podataka modernim sustavima za enkripciju bez poznavanja lozinke za dekriptiranje zbog npr. računalnog napada zlonamjernim programom ransomware ili u slučaju gubitka iste najčešće rezultira potpunim gubitkom podataka, koji nam postaju zauvijek nečitljivi.

6.1. UVODNO O KRIPTOGRAFIJI

Prema Dujella i Maretić (2007) kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. Samo komuniciranje odvija se na način da pošiljatelj (onaj koji generira poruku) šalje poruku primatelju (onaj za koga je poruka namijenjena) putem nekog komunikacijskog kanala. Taj kanal je najčešće nesiguran, osim ako oba subjekta nisu u npr. zatvorenoj zvučno izoliranoj prostoriji. Od samih početaka ljudske komunikacije, postoji želja i potreba za sigurnim komuniciranjem, ali i svjesnost da poruke često putuju nesigurnim kanalima komuniciranja. Osnovni je problem, koji se pokušava riješiti pomoću kriptografije, onemogućiti onoga tko nadzire taj komunikacijski kanal da sazna sadržaj poruke koja se prenosi.



Slika 1.
Shema klasične kriptografije

Osnovni pojmovi koji se koriste u kriptografiji:

- pošiljatelj – osoba koja šalje poruku,
- primatelj – osoba koja prima poruku, za koju je poruka namijenjena,
- protivnik – treća osoba, koja pokušava neovlašteno prisluškivati poruku,
- komuniciranje – razmjena poruka, informacija,
- komunikacijski kanal – put, sredstvo kojim poruka putuje,
- otvoreni tekst – izvorna, nepromijenjena poruka (engl. plaintext),
- ključ - način šifriranja i dešifriranja podataka (engl. key),
- šifriranje – postupak transformacije otvorenog teksta pomoću ključa,

- šifrat/kriptogram – dobiveni rezultat šifriranja (engl. chipertext),
- dešifriranje – postupak transformacije šifrata u otvoreni tekst pomoću ključa,
- kriptografski algoritam – matematička funkcija koja se koristi za šifriranje i dešifriranje,
- prostor ključeva – skup svih mogućih vrijednosti ključeva,
- kriptosustav – sastoji se od kriptografskog algoritma i svih mogućih otvorenih tekstova, šifrata i ključeva.

Kriptoanaliza/dekriptiranje je znanstvena disciplina koja proučava postupke za čitanje šifrata bez poznavanja ključa, a sam postupak se naziva kriptoanalitički napad. Kriptografija i kriptoanaliza zajedno čine kriptologiju.

Dujella i Maretić (2007) klasificiraju kriptosustave prema:

1. Tip operacija koje se koriste pri šifriranju

Supstitucijske šifre – svaki element otvorenog koda zamjenjuje se drugim elementom.

Transpozicijske šifre – elementi otvorenog teksta se permutiraju (premještaju).

2. Način na koji se obrađuje otvoreni tekst

Blokovne šifre - obrađuje se blok po blok elemenata otvorenog teksta koristeći jedan te isti ključ.

Protočne šifre - obrađuje se element po element otvorenog teksta koristeći pri tome niz ključeva (engl. keystream) koji se paralelno generira.

3. Tajnost i javnost ključeva

Simetrični (konvencionalni) kriptosustavi - ključ za dešifriranje se može izračunati poznavajući ključ za šifriranje i obratno. Ti ključevi su najčešće identični. Sigurnost leži u tajnosti ključa.

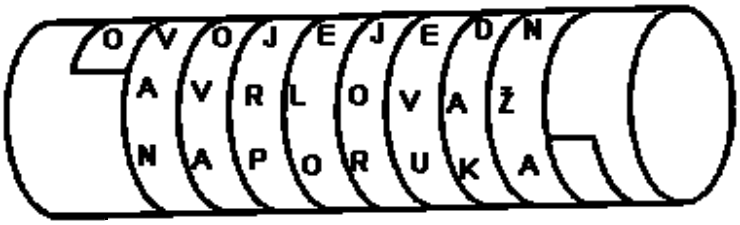
Kriptosustavi s javnim ključem - ključ za dešifriranje se ne može izračunati iz ključa za šifriranje, barem ne u nekom razumnom vremenu. Ključ za šifriranje je javni. Bilo tko može šifrirati poruku pomoću njega, ali poruku može dešifrirati samo osoba koja ima odgovarajući ključ za dešifriranje - privatni (tajni) ključ. Godine 1976. Whitfield Diffie i Martin Hellman su prvi iznijeli ideju javnoga ključa (Dujella i Maretić, 2007).

Osnovna pretpostavka kriptoanalize je da kriptoanalitičar koji pokušava dekriptirati poruku zna koji se kriptosustav koristi. Prema Nizozemcu Augustu

Kerckhoffsu, autoru knjige „Vojna kriptografija“ iz 1883. godine, ovo se naziva Kerckhoffsovo načelo (Dujella i Maretić, 2007). Iako ova pretpostavka ne mora biti točna, sigurnost kriptosustava ne može počivati na pretpostavci da protivnik ne zna koji kriptosustav koristimo.

6.2 POVIJESNI RAZVOJ KRIPTOGRAFIJE

Dujella i Maretić (2007) navode kao jednu od prvih poznatih upotreba kriptografije u staroj Grčkoj, gdje su Spartanci već u 5. stoljeću prije Krista koristili napravu za šifriranje. Naprava se nazivala „skital“, a sastojala se od štapa ili nekog drugog predmeta oko kojega se namotavala vrpca od pergamenta, te se je na nju okomito ispisivala poruka. Nakon razmatanja vrpce, poruka bi bila izmiješana te bi ju mogao pročitati samo onaj tko je imao štap iste debljine. Ovo je osnovni primjer transpozicijske šifre.



Slika 2.
Skital (Dujella, 2018)

6.2.1. SUPSTITUCIJSKE ŠIFRE

Kao jednu od prvih poznatih uporaba supstitucijske šifre Dujella i Maretić (2007) navode zapisivanje Knjige o Jeremiji, kao dijela Biblije, u 6. stoljeću prije Krista kada je korištena jednostavna šifra zasnovana na principu zamjene slova abecede, tzv. Hebrejska šifra. U ovom slučaju, korištena je inačica koja izvrće abecedu naopako, poznata pod imenom ATBASH. Osim „atbash” šifre postoje još „albam” i „atbah” šifra.

Tablica „atbash” šifre za engleski jezik glasi:

A	B	C	D	E	F	G	H	I	J	K	L	M
Z	Y	X	W	V	U	T	S	R	Q	P	O	N

Tablica 1.
Atbash (Dujella, 2018)

Tablica „albam" šifre za engleski jezik glasi:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Tablica 2.
Albam (Dujella, 2018)

Ovakav način kriptiranja je recipročan, tj. ako se prvo slovo zamjeni s drugim, onda se drugo slovo zamjeni s prvim.

6.2.1.1. Cesarova šifra

Najpoznatija supstitucijska šifra, koju je koristio poznati rimski vojskovođa, državnik i car, Gaj Julije Cezar (Dujella i Maretić, 2007). U Cezarovoj šifri, slova otvorenog teksta zamjenjuju se slovima koja se nalaze tri mjesta dalje od njih u alfabetu (A -> D, B -> E, C -> F…) s pretpostavkom da se alfabet ciklički nastavlja, odnosno poslije Z, ponovo dolazi A, B, C.

Cezarovu šifru možemo zapisati u tablici:

Otvoreni tekst	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
šifrat	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Tablica 3.
Cesarova šifra (Dujella, 2018)

A njegova poznata izreka:

VENI VIDI VICI

bila bi šifrirana ovako:

YHQL YLGL YLFL

Radi matematičke obrade i modifikacije originalne Cezarove šifre, te analize pomaka različitih od tri, zamijenit ćemo slova alfabeta s njihovom brojčanom oznakom pozicije Z26 = {0, 1, 2, ... , 25} (skup brojeva 0-25), prema tablici:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Tablica 4.
Zamjena alfabeta brojčanom oznakom (Dujella, 2018)

Cezarovu šifru definiramo na sljedeći način:

$eK(x) = (x + K) \bmod 26,$

$dK(y) = (y - K) \bmod 26.$ mod 26 - ostatak cjelobrojnog dijeljenja sa 26

Originalna Cesarova šifra ima ključ K=3, odnosno pomicanje alfabeta za točno tri mjesta udesno. Poznavajući kriptosustav (Kerckhoffsovo načelo) i ključ, vrlo je jednostavno otvoreni tekst pretvoriti u šifrat i obrnuto. Problem nastaje kada nam je K nepoznat.

Primjer 1: Potrebno je dekriptirati šifrat TXNOJP dobiven Cezarovom šifrom.

Budući da nam je nepoznat ključ šifriranja, morat ćemo pristupit kriptoanalizi. Prostor ključeva (skup svih mogućih vrijednosti ključeva) je mali (ima ih samo 26, odnosno 25 budući da bi korištenje ključa 0/26 dalo identičan otvoreni tekst i šifrat) te ovaj problem možemo riješiti takozvanom „grubom silom" (engl. „brute force"). Napad grubom silom na šifrat je napad pri kojemu isprobavamo sva moguća rješenja dok ne nađemo odgovarajuće. U našem slučaju, imamo šifrat, pa isprobavamo redom ključeve K=1,2,3… dok ne nađemo neki koji nam daje smisleni tekst.

T	X	N	O	J	P
S	W	M	N	I	O
R	V	L	M	H	N
Q	U	K	L	G	M
P	T	J	K	F	L
O	S	I	J	E	K

Tablica 5.
Dekriptiranje korištenjem grube sile

Znači, ključ je K=5, a otvoreni tekst je OSIJEK.

Kao što se primjećuje, Cesarova šifra uz jednostavni ključ je vrlo jednostavna za dekriptiranje. Da bismo dobili malo sigurniju šifru, u funkciju za šifriranje trebamo uključiti više od jednog parametra te koristimo slijedeću afinu funkciju: $f(x)=ax+b$ uz uvjet da je parametar a prost broj unutar skupa mod(26), kao i njegov multiplikativni inverz a^{-1}.

Tablica vrijednosti parametra a i multiplikativnog inverza a^{-1} u skupu Z_{26}:

a	1	3	5	7	9	11	15	17	19	21	23	25
$\mathbf{a^{-1}}$	1	9	21	15	3	19	7	23	11	5	17	25

Tablica 6.
Vrijednosti parametra *a* i multiplikativnog inverza a^{-1} (Dujella, 2018)

Primjer 2: Potrebno je šifrirati otvoreni tekst OSIJEK uz K=(5,3)

Zamjenjujući slova OSIJEK s njihovim vrijednostima prema ranije navedenoj Tablici 4. (14,18,8,9,4,10) te korištenjem K=(5,3) -> a = 5; b = 3 dobijemo:

14x5 + 3 = 73, 73 mod 26 = 21
18x5 + 3 = 93, 93 mod 26 = 15
8x5 + 3 = 43, 43 mod 26 = 17
9x5 + 3 = 48, 48 mod 26 = 22
4x5 + 3 = 23, 23 mod 26 = 23
10x5 + 3 = 53, 53 mod 26 = 1

Odnosno šifrat VPRWXB.

Primjer 3: Potrebno je dekriptirati šifrat OZWHRYEZCVWFCTPCUWRCF-PYHWI dobiven afinom šifrom

U svojoj knjizi, Dujella i Maretić (2007) opisuju da afina funkcija f(x)=ax+b ima ukupno 12 permutacija za vrijednost a te 26 za vrijednost b, ukupno je moguće 12x26=326 ključeva. Iako je i ovdje moguće primijeniti „brute force" napad, postoji i puno elegantniji način za dekriptiranje. Ukoliko znamo kojim je jezikom pisan otvoreni tekst, moguće je prema frekvenciji slova „pogoditi" ključ. Najfrekventnija slova u hrvatskom jeziku su A, I, O, E, N, dok je u šifratu najzastupljenije C i W (4 puta).

$e_K(A) = ax0+b=b$, $e_K(I) = 8a+b$

Ako pretpostavimo da je $e_K(A) = C$, a $e_K(I) = W$, dobijemo b=2 i a=9, te otvoreni tekst glasi:

KRIPTOGRAFIJA ZNACI TAJNOPIS

Cezarova i afina funkcija su specijalni slučajevi supstitucijske šifre. Prostor ključeva K može se sastojati od svih permutacija skupa skupa {0, 1, 2, ... , 25} gdje je

$e_\pi(x) = \pi(x)$, $d_\pi(y) = \pi^{-1}(y)$,

gdje je π^{-1} inverzna permutacija od π.

U ovom slučaju, imamo 26! mogućih ključeva (1x2x3x4…x26), što je $\approx 4x10^{26}$ kombinacija, te je napad korištenjem grube sile praktički nemoguć. Ovdje se kod dekriptiranja koristi kao osnovna metoda analiza frekvencije slova. Broji se pojavljivanje svakog slova u šifratu, te se distribucija slova u šifratu uspoređuje s poznatim podatcima o distribuciji slova u jeziku otvorenog teksta. Vrlo je vjerojatno da najfrekventnija slova šifrata odgovaraju najfrekventnijim slovima jezika. Ta vjerojatnost raste s duljinom šifrata. Također mogu biti korisni i podatci o najčešćim bigramima (parovima slova) i trigramima (nizovima od tri slova) u jeziku.

FREKVENCIJA SLOVA (u promilima)				
A	115		K	36
I	98		V	35
O	90		L	33
E	84		M	31
N	66		P	29
S	56		C	28
R	54		Z	23
J	51		G	16
T	48		B	15
U	43		H	8
D	37		F	3

Tablica 7.
Frekvencije pojedinih slova (Dujella, 2018)

Najfrekventnija slova u engleskom jeziku su: E, T, A, O, I, N, S, R, H, L; u njemačkom jeziku: E, N, I, R, S, A, T, D, H, U, a u francuskom E, A, I, S, T, N, R, U, L, O.

Najfrekventniji bigrami u hrvatskom jeziku su: JE (2,7 %), NA (1,5 %), RA (1,5 %), ST, AN, NI, KO, OS, TI, IJ, NO, EN, PR (1,0 %).

Iako postoji veliki broj ključeva, supstitucijska šifra pokazala se vrlo jednostavnom za kriptoanalizu.

6.2.1.2. Vigenèreova šifra

Osnovni problem supstitucijske šifre je što svakom slovu otvorenog teksta odgovara jedno slovo šifrata. To je tzv. monoalfabetska šifra. Kako bi se pojačala sigurnost u 16. stoljeću počinju se koristiti polialfabetske šifre. Kod njih se svako slovo otvorenog teksta može preslikati u jedno od *m* mogućih slova, gdje je *m* duljina ključa. Prema Dujella i Maretić (2007) ovu vrstu šifriranja prvi je opisao francuski diplomat Vigenère 1586. godine, te se ta vrsta šifriranja po njemu naziva *Vigenèreova šifra* (Dujella, 2018).

Pojednostavljeno, ključ nije broj kojim se množi ili zbraja, već je to riječ, koja pretvorena u numerički ekvivalent tvori niz brojeva. Ako je ključna riječ OSIJEK (m=6) numerički ekvivalent je ključ K=(14,18,8,9,4,10). Ukoliko je ključna riječ kraća od otvorenog teksta, a gotovo uvijek u pravilu jeste, ona se jednostavno ponavlja koliko puta treba. Ako želimo šifrirati otvoreni tekst HRVATSKA, čiji je numerički ekvivalent (7,17,21,0,19,18,10,0) šifriranjem dobijemo:

	14	18	8	9	4	10	14	18
+	7	17	21	0	19	18	10	0
Mod26	21	9	3	9	23	2	24	18

Tablica 8.
Šifriranje riječi HRVATSKA - numerički ekvivalent

Odnosno:

Ključ	O	S	I	J	E	K	O	S
Otvoreni tekst	H	R	V	A	T	S	K	A
šifrat	V	J	D	J	X	C	Y	S

Tablica 9.
Šifriranje riječi HRVATSKA - numerički ekvivalent

Primjećujemo da se prvo slovo A iz otvorenog teksta preslikalo u J, a posljednje A u S. Ovime se izbjegava mogućnost kriptoanalize na temelju frekvencije pojave slova, bigrama i trigrama. Ovakva vrsta šifri naziva se blokovna šifra, budući da se ključ šifriranja pojavljuje (ponavlja) u blokovima. Postoje i druge varijante Vigenèreove šifre, kao npr. s autoključem (engl. Autokey), u kojoj se originalni ključ koristi samo za šifriranje prvog bloka (od *m* znakova), a dalje se koristi prethodni blok otvorenog teksta. U našem primjeru, za prvih šest znakova koristio bi se originalni ključ OSIJEK, dok bi se za posljednja dva koristio početak otvorenog teksta HR.

Dujella i Maretić (2007) navode Vigenèreova šifru kao jedan je od najdugovječnijih i najpopularnijih kriptosustava u povijesti. Koristila se intenzivno tijekom Američke revolucije te Američkog građanskog rata.

Iako na prvi pogled ovu šifru izgleda gotovo nemoguće za probiti, što je čak objavljeno i u časopisu „Scientific American" 1917. godine, već krajem 19. stoljeća započeli su procesi koji će dovesti do njenog uspješnog dekriptiranja. Prvi korak je određivanje duljine ključne riječi (Dujella i Maretić 2007).

Pretpostavka je da će dva identična odsječka otvorenog teksta biti šifrirana na isti način ukoliko se njihove početne pozicije razlikuju za neki višekratnik od m (koristit će kao ključ isti dio ključne riječi). Posljedično, ako uočimo dva identična odsječka u šifratu, duljine barem tri (odsječci duljine 2 često budu slučajni), tada je vrlo vjerojatno da oni odgovaraju identičnim odsječcima otvorenog teksta. U šifratu tražimo parove identičnih odsječaka (duljine barem 3), te zabilježimo udaljenosti između njihovih početnih položaja. Većina udaljenosti između ovih parova trebala bi biti djeljiva s m, odnosno nekim njegovim višekratnikom. Ova metoda zove se Kasiskijev test, a uveo ju je Friedrich Kasiski 1863. godine (Dujella i Maretić 2007).

Nakon saznanja duljine ključa *m*, pristupa se metodi indeksa koincidencije. Sama metoda opisana je u knjizi Dujella i Maretić (2007), a sastoji se u tome da se šifrat stavi u matricu s *m* stupaca, te se iščitava učestalost pojavljivanja određenog slova u pojedinom stupcu šifrata, budući da smo cijelu Vigenèreovu šifru zapravo rastavili na *m* Cesarovih šifri. Valja napomenuti da za uspjeh u rješavanju šifri nije bitna sposobnost da se poznaje jezik originalnog teksta, mada je barem poželjna sposobnost pisanja.

6.2.1.3. Polialfabetska šifra - Playfairova šifra

Dujella i Maretić (2007) iznose da osnovna ideja ovog načina šifriranja jeste da umjesto šifriranja slova, šifriramo blokove slova od dva elementa (bigrami).

Problem realizacije ove ideje je da umjesto 26 elemenata imamo 26 x 26 blokova, odnosno 676 elemenata otvorenog teksta. Algoritam za šifriranje bazira se na matrici 5 x 5 slova, koja se konstruira koristeći ključnu riječ, a dalje se upisuju redom preostala slova alfabeta. Ako je ključna riječ OSIJEK, matrica izgleda ovako:

O	S	I	J	E
K	A	B	C	D
F	G	H	L	M
N	P	R	Q	T
U	VW	X	Y	Z

Tablica 10.
Izrada Playfairove matrice – ključna riječ OSIJEK

Budući da matrica ima 25 znakova, a alfabet 26, u engleskom jeziku slova I i J se poistovjećuju, odnosno jednako šifriraju. U hrvatskom jeziku, da bi izbjegli moguće nesporazume, poistovjećujemo slova V i W.

Šifriranje se provodi na sljedeći način. Prvo se blokovi otvorenog teksta podijele na blokove po dva slova, pazeći da se ni jedan blok ne sastoji od dvaju istih znakova i da je ukupna duljina teksta parna! Oboje postižemo umetanjem slova X gdje je potrebno. Šifriranje se dalje obavlja slijedeći tri pravila, ovisno o položaju slova u dobivenoj matrici. Kao primjer, koristimo otvoreni tekst SLAVONIJA, odnosno šifriramo parove SL AV ON IJ AX

1. Ako se slova nalaze u istom retku, mijenjamo ih sa slovima koja se nalaze jedno mjesto udesno. Ukoliko dođemo skroz do kraja desno, nastavljamo od početka reda, s lijeve strane. IJ -> JE

2. Ako se slova nalaze u istom stupcu, mijenjamo ih sa slovima koja se nalaze jedno mjesto ispod. Ukoliko dođemo skroz do kraja dolje, nastavljamo od početka stupca, s gornje strane. ON -> KU, AV -> GS

3. Ako nije zadovoljen niti jedan gore navedeni uvijek, gledamo pravokutnik koji tvore slovate ih zamjenjujemo sa slovima s preostala dva kuta tog pravokutnika. Redoslijed određujemo tako da uzmemo prvo ono slovo koje je u istom retku kao i prvo slovo u našem bloku. SL – JG, AX -> BV

Kriptiranjem otvorenog teksta SLAVONIJA pomoću Playfairove šifre s ključem OSIJEK dobijemo šifrat JGGSKUJEBV.

Dujella i Maretić (2007) navode kako je Playfairovu šifru smislio britanski znanstvenik Charles Wheatstone 1854. godine, a ime je dobila po barunu Playfa-

iru koji ju je popularizirao. Ova vrsta šifre ima nekoliko značajnih prednosti pred monoalfabetskom supstitucijskom šifrom. Budući da je bigramska (blokovi od 2), u šifratu se gube jednoslovne riječi („a", „i" „u") koje znatno utječu na frekvenciju. Broj bigrama je 676, što je znatno više od standardnih 26 individualnih slova, a i njihova frekvencija pojavljivanja je znatno ujednačenija. Zbog svega toga, dugo vremena se smatrala sigurnom i korištena je kao standardna šifra u britanskoj vojsci za vrijeme prvog svjetskog rada, a čak u nekim slučajevima i kasnije.

Ipak, i ova šifra nije u potpunosti sigurna. Kod dugih tekstova šifra postaje nesigurna jer se može koristiti analiza frekvencije bigrama. U otvorenom tekstu najfrekventnije slovo u engleskom jeziku ima učestalost oko 13%, u šifratu dobivenom Playfairovom šifrom ona iznosi oko 7%. Također, postoji i metoda vjerojatne riječi, koja nam omogućava da pokušamo pogoditi visokofrekventne bigrame (Dujella i Maretić, 2007).

6.2.1.4. Hillova šifra

Godine 1929. Lester Hill predložio je poligramsku šifru kod koje se *m* uzastopnih slova otvorenog teksta zamjenjuje s *m* slova u šifratu. Za upotrebu ključa preporučio je upotrebu invertibilne matrice (Dujella i Maretić, 2007). Ovaj sustav, već s matricama 3 x 3 skriva ne samo frekvencije slova, nego i frekvencije bigrama. Korištenje matrica s $m \geq 5$ čini ovaj sustav gotovo potpuno sigurnim.

Ipak, ovu šifru je vrlo lako razbiti pomoću napada „poznati otvoreni tekst". Kod ovog napada, uspoređuje se poznati tekst koji nije kriptiran sa svojim šifratom te se iz toga u ovom slučaju može jednostavno saznati ključ. Za ovaj napad potrebno je imati jednu šifriranu poruku i njezin otvoreni tekst. Poznavanjem ključa moguće je čitati sve daljnje poruke nastale njegovim korištenjem.

6.2.1.4. Jednokratna bilježnica

U želji za definiranjem savršeno sigurnog kriptosustava, zaključeno je da je isti moguć samo uz uvjet da šifrat ne daje nikakvu informaciju o otvorenom tekstu. Dujella i Maretić (2007) iznose da je to moguće ako i samo ako je svaki ključ korišten s istom vjerojatnošću i da za svaki šifrat postoji jedinstveni ključ. Realizacija toga je tzv. jednokratna bilježnica. Ovaj sustav ne radi sa slovima, već bitovima (nule i jedinice), a otvoreni tekst, šifrat i ključ su nizovi bitova duljine n. Budući da je postupak šifriranja jednostavno zbrajanje bitova otvorenog teksta i ključa, sustav je vrlo lako razbiti napadom „poznati otvoreni tekst". Sigurnost ovog sustava postiže se samo ako se svaki ključ koristi samo jedanput. Također, problem predstavlja i to što ključ mora biti jednako dug kao i sama poruka.

6.2.2. TRANSPOZICIJSKE ŠIFRE

Kao što smo već naveli, transpozicijske šifre su one kod kojih ne mijenjamo elemente otvorenog teksta, već im mijenjamo međusobni položaj. Najupotrebljavanija transpozicijska šifra u praksi bila je stupčana transpozicija. Otvoreni tekst upisuje se u pravokutnik po recima, a poruka se čita po stupcima, ali s promijenjenim poretkom prema ključu. Kao i kod ostalih šifri, ukoliko se posljednji redak ne popuni do kraja, prazna mjesta se pune proizvoljnim slovima.

Šifriranje otvorenog teksta:

INFORMACIJSKA SIGURNOST I PRIVATNOST

Stupčanom transpozicijom s ključem: 5 2 7 4 1 3 6

ključ	5	2	7	4	1	3	6
	I	N	F	O	R	M	A
otvoreni	C	I	J	S	K	A	S
tekst	I	G	U	R	N	O	S
	T	I	P	R	I	V	A
	T	N	O	S	T	X	W

Tablica 11.
Šifriranje izraza: INFORMACIJSKA SIGURNOST I PRIVATNOST

Šifrat je:

RKNITNIGINMAOVXOSRRSICIITASSAWFJUPO

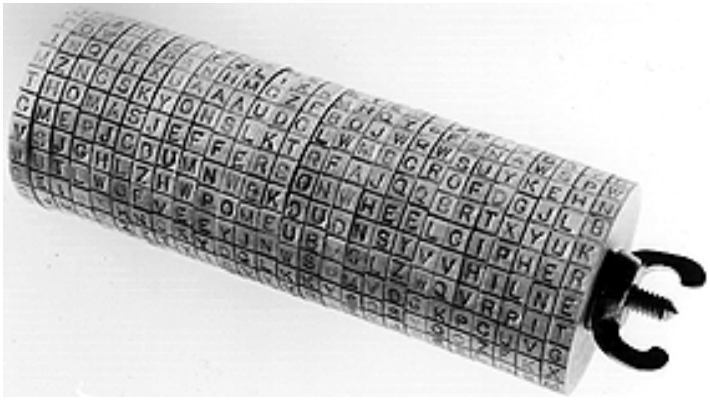
Dekriptiranje transpozicijske šifre provodise tako da se prvo odredi dimenzija pravokutnika. Broj slova u šifratu se faktorizira i dobijemo nekoliko odgovarajućih dimenzija. U našem slučaju to je 35, odnosno 5x7 i 7x5. Da bi se odredio ispravni format, promatra se odnos samoglasnika i suglasnika u svakom retku. Prema Dujella i Maretić (2007), taj odnos bi trebao biti blizak odnosu u jeziku otvorenog teksta (u hrvatskom 43% : 57%) Nakon utvrđivanja ispravnog oblika, stupce možemo pokušati anagramirati ili možemo pokušati koristiti frekvencije najčešćih bigrama između parova stupaca. Oni parovi stupaca koji imaju najveće vrijednosti, vjerojatno se nalaze jedan pored drugoga.

6.2.3. NAPRAVE ZA ŠIFRIRANJE

Upotrebom naprava za šifriranje kriptosustavi se mogu učiniti kompliciranijima i sigurnijima. Te naprave čine proces šifriranja i dešifriranja bržim, a prostor ključeva većim.

6.2.3.1. Jeffersonov kotač

Jedna od prvih korištenih naprava bio je Jeffersonov kotač za šifriranje. Sastojao se od cilindra na kojemu se nalazilo 26 diskova, svaki s 26 kvadratića na kojima se proizvoljno nalaze slova engleskog alfabeta. Ti diskovi mogu se neovisno rotirati. Šifriranje se obavlja tako da se na jednom retku dobije otvoreni tekst, a kao šifrat se koristi bilo koji od preostalih 25 redaka (Dujella i Maretić, 2007).



Slika 3.
Jeffersonov kotač za šifriranje (University of Virginia, 2005)

Dešifriranje se obavlja tako da se rotiranjem diskova u jednom retku dobije šifrat. Sada se između preostalih 25 redaka potraži onaj koji sadrži neki smisleni tekst i taj redak predstavlja otvoreni tekst.

6.2.3.2. Hebernov električni stroj za kodiranje

Dujella i Maretić (2007) opisuju električni uređaj kojim su se dva električna pisača stroja spajala pomoću 26 žica, ali s razbacanim rasporedom. Pritiskom na tipku na pisaćem stroju za otvoreni tekst, drugi bi stroj otipkao šifrat tog slova. Dvije godine kasnije, u uređaj je ugradio pet tzv. „rotora". Rotori su na svakoj strani imali po 26 električnih kontakata, a okretanje rotora mijenjalo je nasumične spojeve s kontaktima na drugoj strani. Korištenje pt rotora omogućavalo je polialfabetsku supstituciju s 26^5 kombinacija, odnosno nešto više od 11 milijuna.

6.2.3.3. ENIGMA

Slika 4.
ENIGMA (Wikipedija)

Dujella i Maretić (2007) navode kako je Arthur Scherbius, njemački inženjer, izradio i patentirao 1918. godine ENIGMA uređaj, rotorsku mašinu s mogućnošću kodiranja i prijenosa poruka. Za razliku od ostalih rotorskih naprava, ENIGMA je imala tri, odnosno prt zupčanika koji su rotore mogli pomicati u nepravilnom slijedu. Neposredno pred Drugi svjetski rat započelo je njezino masovno korištenje u njemačkoj vojsci i mornarici, te je tako nastao najpoznatiji stoj za šifriranje. Enigma je bila elektromehanička naprava koja je imala tipkovnicu s 26 tipki za unos teksta, zaslon s 26 žaruljica koje su prikazivale šifrirani izlaz, tri (kasnije 5) mehaničkih rotora i električne prespojne ploče. Rotori su bili smješteni tako da se kontakti među njima dodiruju, tako da je izlaz iz jednoga bio ulaz u drugi. Nakon svakog šifriranog slova, prvi rotor bi se okrenuo za jedan kontakt, a kad bi načinio potpuni krug uzrokovao bi okretanje slijedećeg rotora. Na taj način, kodiranje istog slova otvorenog teksta nikada nije završavalo istim šifratom te je stoga frekvencijska analiza bila neprikladna. Tri rotora s 26 kontakata daju 26^3 kombinacija, odnosno 17576.

Kako bi se povećala sigurnost, korišteni su izmjenjivi rotori i prespojni kablovi. Mehanički identični rotori imali su različite električne spojeve te su međusobnom zamjenom mjesta omogućavali 3! = 6 permutacija. Prespojna ploča omogućavala je zamjenu nekih slova prije ulaska u prvi rotor. U početku se koristilo šest prespojnih kablova, a kasnije 10. Kod korištenja šest kablova ukupan broj kombinacija je veći od 100 milijardi, a kod 10 kabela veći od 150.000 milijardi, što čini

„brute force“ napad nemogućim. Proboj u kriptoanalizi ENIGME omogućilo je poznavanje procedure šifriranja te jedna nehotična pogreška u proceduri koja je korištena kako bi se osigurala ispravnost primljene poruke.

Šifriranje se odvijalo na sljedeći način. Svaki mjesec, operaterima ENIGME bila je dostavljana nova knjiga s ključevima za svaki dan u tom mjesecu. Ključevi su se sastojali od tri dijela: postavke na prespojnoj ploči, raspored rotora i početne orijentacije rotora. Budući da su se dnevno šifrirale velike količine poruka, kako bi se osigurala jedinstvenost ključa, na početku poruke slan je ključ za samu poruku šifriran pomoću dnevnog ključa. Tako su sve poruke slane taj dan imale iste postavke prespojne ploče, isti raspored rotora, ali različitu orijentaciju. Sukladno dnevnom ključu, pošiljatelj bi odabrao novu orijentaciju za ključ i uvrstio je u šifrat na početku poruke, ali dvaput, kako bi bio siguran da je primatelj dobio ispravan ključ. Ostatak poruke šifrirao bi se korištenjem nove orijentacije. Primatelj bi šifrat koji bi dobio dešifrirao koristeći dnevni ključ za prvih 6 slova šifrata, a za ostalo bi koristio novodobiveni ključ za poruku. Upravo ovo ponavljanje (1=4, 2=5, 3=6) korišteno je za kriptoanalitički napad na ENIGMU (World Science Festival, 2013).

6.2.3.4. BOMBA

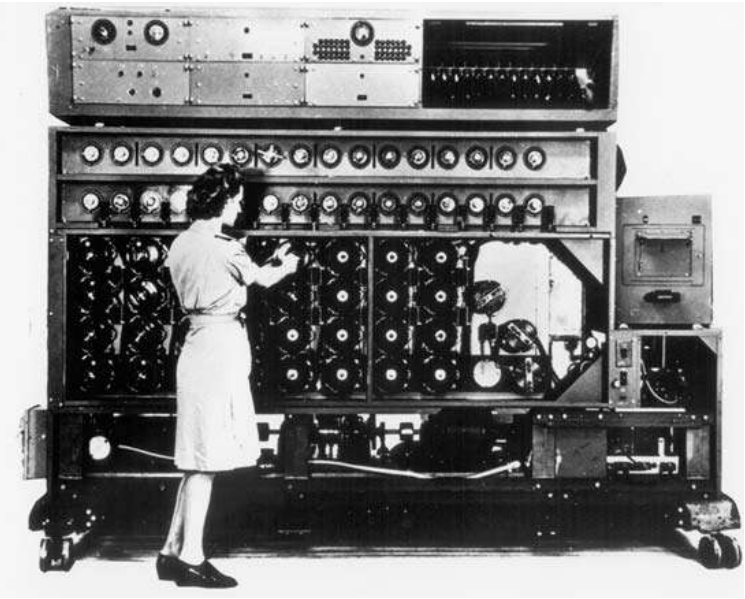
Britanska vojna obavještajna (MI-6) služba dugo je vremena, još od početka Prvog svjetskog rata, uspješno presretala i dešifrirala Njemačke vojne, diplomatske i komercijalne poruke (Kahn, 1979). Dolaskom nacista na vlast važnost tajnovitosti ističe se u prvi plan te 1934. godine njemačke vlasti počinju mijenjati šifriranje s novim sustavom. Više od četiri godine britanske službe tapkale su u mraku, dok 1938. godine nisu saznali da se njemačka vojska koristi uređajem za šifriranje zvanim ENIGMA.

Prvi proboj u dešifriranje ENIGME napravili su poljski matematičari M. Rajewski i H. Zygalski (Copeland, 2010), na temelju ranije opisanih njemačkih uputa za uporabu ENIGME, koje je nabavila francuska obavještajna služba. Koristeći dupliranje ključa na početku njemačkih poruka, počeo je osmišljavati metodu za probijanje ENIGME. Ako je ključ ABC, zapisan je dvaput kao ABCABC i šifriran u npr. FOESCG, Rejewski zaključuje da su F i S šifrat istog slova A, kao i parovi (O,C) i (E,G), kako što opisuje Hrvoje Čavrak, Hrvatski matematički elektronski časopis, http://e.math.hr/enigma/index.html. Ovo ponavljanje omogućilo je Poljacima da detektiraju uzorke i lance sljedivosti slova te da dužina lanaca ne ovisi o prespojnim pločama, već isključivo o postavkama rotora. Stoga, umjesto 150.000 milijardi kombinacija, nakon godinu dana kategorizacije, popisano je svih 105.456 mogućih kombinacija rotora. Svakog dana, nakon dovoljnog broja

prikupljenih poruka i uočenih lanaca, Rejewski je pomoću svoje baze podataka o postavkama, postavke rotora i rezultirajućih lanaca u njima, pronašao odgovarajući. Time je otkrio postavke dnevnih postavki rotora, a rješavanje prespojne ploče, koja može imati milijarde prespojnih kombinacija, svelo se na problem obične supstitucijske šifre. Nakon što su Nijemci 1939. godine dodali još dva rotora u uređaj ENIGME, povećali broj prespojnih kablova na 10 te prestali ključeve u poruci slati dvaput, dešifriranje ENIGME opet je bilo onemogućeno. Neposredno pred napad Njemačke na Poljsku, Poljaci su poslali Britancima svu dokumentaciju vezanu za ENIGMU.

Brown (1975) opisuje kako su Britanci već imali odjel za kriptoanalizu smješten u Bletchley Parku, koji je postao sjedište savezničkih nastojanja za dešifriranje ENIGME. Mladi engleski matematičar Alan Turing osmislio je „Univerzalni stroj", uređaj koji je mogao simulirati rad bilo kojeg drugog uređaja. Iako su govorili da je izgradnja takvog uređaja nemoguća, da bi bio velik kao katedrala Sv. Pavla, da bi zahtijevao da cijelo sveučilište samo obučava radnike za njegovo održavanje te da bi trebala jedna hidroelektrana za njegovo napajanje, Alan Turing nije odustajao te je 1938. godine napravljena BOMBA veličine 2,5 x 2,5 metra.

Traženje lanaca slijedivosti slova, koje su Poljaci ručno uspoređivali s bazom, za Britance je obavljao stroj BOMBA, a sve takve poruke dobivene kriptoanalizom bile su označene kao poruke ULTRE.



Slika 4.
BOMBA, uređaj za dekriptiranje ENIGME - Encyclopedia Britannica

6.2.3.5. Važnost kriptoanalize

Brown (1975) pojašnjava kako je omogućavanje Britanaca da čitaju gotovo sve poruke njemačke vojske, mornarice i zrakoplovstva bilo je ključno za zaustavljanje nacističke Njemačke. Rommel je u Africi pobijeđen kada je ostao bez goriva i municije. U očajničkom pokušaju dostave municije i goriva tijekom prijelomnih trenutaka uoči bitke za El Alamein, pet brodova isplovilo je iz pet talijanskih luka tijekom noći, no zahvaljujući porukama ULTRE svih pet brodova su presreli britanski razarači i potopili ih. Zaustavljanje njemačkih podmornica i osiguravanje pomorskih linija, također je jedna od zasluga ULTRE. Dan D, savezničko iskrcavanje u Francuskoj omogućile su obmane i čitanje poruke njemačke vrhovne komande. Poruke ULTRE bile su najvažniji događaj na putu poraza nacističke Njemačke.

6.2.4. MODERNI SIMETRIČNI BLOKOVNI KRIPTOSUSTAVI

Kao što smo već rekli, simetrični sustavi su oni kod kojih se ključ za dešifriranje može izračunati poznavajući ključ za šifriranje i obratno. Ti ključevi su najčešće identični, a sigurnost leži u tajnosti ključa.

Krajem 60-ih i početkom 70-ih godina 20. stoljeća, razvojem financijskih transakcija, pojaviljuje se potreba za šifrom koju će moći koristiti korisnici širom svijeta i u koju će svi oni moći imati povjerenje.

Dujella i Maretić (2007) opisuju kako je 1972. godine američki National Bureau of Standards (NBS) inicirao je program za zaštitu računalnih i komunikacijskih podataka, čiji je jedan od ciljeva bilo i razvijanje standardnog kriptosustava koji je trebao zadovoljiti sljedeće uvjete:

- visoki stupanj sigurnosti,
- potpuna specifikacija i lako razumijevanje algoritma,
- sigurnost leži u ključu, a ne u tajnosti algoritma,
- dostupnost svim korisnicima,
- prilagodljivost uporabi u različitim primjenama,
- ekonomičnost implementacije u elektoničkim uređajima,
- učinkovitost,
- mogućnost provjere,
- mogućnost izvoza (zbog američkih zakona).

6.2.4.1. Data Encryption Standard (DES)

DES je nastao na osnovi zahtjeva NBS-a, a zasnivao se na specijalnoj vrsti blokovske šifre - Feistelovoj šifri. Osnovnu ideju iznio je tim kriptografa IBM-a, a doradila ju je NSA. Kao standard, prihvaćen je 1976. godine kada je dobio i ime. Dujella i Maretić (2007) opisuju da je glavna ideja upotreba supstitucija i transpozicija kroz više iteracija. DES šifrira otvoreni tekst duljine 64 bita koristeći ključ K duljine 56 bitate dobija šifrat duljine 64 bita. Procedura se sastoji od tri etape:

1. permutiranje otvorenog teksta pomoću fiksne inicijalne permutacije,
2. primjena F funkcije (16 rundi iteracija),
3. inverzna permutacija dobivenog međuteksta.

Koraci 1 i 3, permutacija i inverzna permutacija, osiguravaju da se isti čip i isti algoritam koriste i za kriptiranje i dekriptiranje. F funkcija, koja se sastoji od osam supstitucijskih S kutija, provodi se 16 puta, kako bi se izrazio tzv. lavinski učinak. Lavinski učinak označava zahtjev da svaka, pa i najmanja promjena ulaznih vrijednosti, rezultira velikom promjenom izlaznih vrijednosti. Ukoliko isti otvoreni tekst šifriramo s pomoću dvaju ključeva koji se razlikuju samo u jednom bitu, dobivamo razlike prema tablici:

Runda	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Broj bitova koji se razlikuju	0	2	14	28	32	30	32	35	34	40	38	31	33	28	26	34	35

Tablica 12.
Razlike u šifriranju otvorenog teksta

Budući da je učinak lavine izražen već kod tri iteracije, 16 rundi se koristi iz razloga da kriptoanalitički napad ne bude učinkovitijiod napada grubom silom. Budući da je ključ 56-bitni, postoji 2^{56} ključeva, odnosno $7{,}2 \times 10^{16}$. Pretpostavljalo se da će do 1990. godine DES postati nesiguran, budući da bi se razvojem računala moglo u razumnom vremenu isprobati sve kombinacije ključa. Prvi puta, DES je razbijen 1998. godine računalom koje je koštalo 250.000 $, a trebalo mu je 56 sati za dekriptiranje poruke.

Kao prijelazno rješenje zaštite podataka 1990-ih godina pojavila se ideja povećanja duljine ključa, te se počeo koristiti trostruki DES. Iako je njegova dulji-

na ključa 3x56=168 bita, zbog mogućnosti tzv. napada u sredini, broj potrebnih operacija napada je 2^{112}, odnosno $5x10^{33}$.

6.2.4.2 Advanced Encryption Standard (AES)

Dujella i Maretić (2007) navode „Napredni standard za enkripciju" (AES) kao glavni standard koji se danas koristi za zaštitu podataka od nedopuštenog pristupa i enkripciju podataka. Ključ koji se koristi za kriptiranje podataka može biti različitih duljina. Ovisno o duljini ključa postoje AES-128, AES-192 ili AES-256. Umjesto Feistelove F funkcije AES koristi substitucijsko-permutacijsku mrežu. Razvili su ga Belgijanci Daemen i Rijmen, kao RIJNDAEL sustav, a nakon prihvaćanja kao standarda, promijenio je ime u AES. S kutije su dizajnirane tako da kriptosustav bude što otporniji na tzv. diferencijalnu i linearnu kriptoanalizu.

6.2.5. ASIMETRIČNI KRIPTOSUSTAVI

6.2.5.1. Kriptografija pomoću javnog ključa

Dujella i Maretić (2007) opisuju ideju javnog ključa, koja se sastoji u tome da se konstruira kriptosustav kod kojega bi iz poznavanja funkcije šifriranja bilo nemoguće izračunati funkciju dešifriranja. Tada bi funkcija šifriranja mogla biti javna.

Kriptiranje se obavlja na način da ako pošiljatelj A želi poslati poruku x primaocu B, onda B najprije pošalje A svoj javni ključ e_B, potom A šifrira svoju poruku pomoću e_B i pošalje primaocu šifrat $y = e_B(x)$. Konačno, B dešifrira šifrat koristeći svoj tajni ključ za dekriptiranje d_B.

Glavne prednosti kriptosustava s javnim ključem u usporedbi sa simetričnima su:

- nema potrebe za sigurnim komunikacijskim kanalom za razmjenu ključeva,
- za komunikaciju grupe od N ljudi treba 2N ključeva, za razliku od N(N-1)/2 ključeva kod simetričnog kriptosustava,
- mogućnost potpisa poruke.

Osnovni razlog zašto se javni ključ ne koristi za šifriranje poruka, jest da su algoritmi s javnim ključem puno sporiji (oko 1000 puta) od modernih simetričnih algoritama. Drugi nedostatak kriptosustava s javnim ključem jest da su slabi na napad „odabrani otvoreni tekst".

U realnom svijetu kriptografija javnog ključa ne predstavlja zamjenu za simetrične kriptosustave. Ona se ne koristi za šifriranje poruka, već za šifriranje

ključeva. Naime, osobe A i B komuniciraju pomoću simetričnog kriptosustava s ključem koji su razmijenili pomoću kriptosustava s javnim ključem. To se zove hibridni kriptosustav.

U modernoj kriptografiji, koja se koristi u komercijalnom svijetu (tipična situacija je da osoba A želi kupiti nešto od osobe B preko interneta), pojavljuju se, uz klasične, i neki sasvim novi problemi:

- POVJERLJIVOST (confidentiality): Poruku koju osoba A šalje osobi B ne može pročitati nitko drugi.
- VJERODOSTOJNOST (autenticity): Osoba B zna da je samo osoba A mogla poslati poruku koju je ona upravo primila.
- NETAKNUTOST (integrity): Osoba B zna da poruka koju je poslala osoba A nije promijenjena prilikom slanja.
- NEPOBITNOST (non-repudiation): Osoba A ne može kasnije zanijekati da je poslala poruku.

6.3. KRIPTOGRAFIJA U PRAKSI

Neki od primjera današnje primjene kriptografije su svakako internetsko bankarstvo koje koristi sve veći broj korisnika interneta; zatim tu su različite kriptovalute od kojih je najpoznatija i najrasprostranjenija - Bitcoin; te izrazito opasan zloćudni računalni program *Cryptoloker* koji predstavlja trenutno najpoznatiju vrstu *ransomwarea*, programa koji zaključavaju korisničke podatke i traže za njih otkupninu.

6.3.1. INTERNETSKO BANKARSTVO

Internetsko bankarstvo odvija se putem nesigurnog medija (interneta) koji je moguće neovlašteno prisluškivati.. Zbog toga, sva komunikacija obavlja se putem https protokola koji kriptira komunikaciju na oba kraja. Sustav kriptiranja je ranije opisani AES, a razmjena ključeva obavlja se putem kriptografije javnog ključa (Certifikat na kartici korisnika). Ovaj način smatra se sigurnijim nego razmjena autorizacijske lozinke putem tokena banke.

Budući da se autorizacija u sustav banke provodi putem korisničkog certifikata koji se aktivira PIN-om, zbog sigurnosti preporučuje se vađenje kartice s certifikatom kada se ne koristi. Budući da postoje neželjeni programi koji vam se mogu instalirati na računalo te pratiti i sve unose na tipkovnici te u pozadini sami pokrenuti neku bankovnu transakciju, u posljednje vrijeme se preferira i

2FA (Two Factor Authentication - autentifikacija u dva koraka). To obično traži dodatni uređaj (mobitel, dodatni token ili sl.) na koji se šalje jednokratna lozinka za autentifikaciju. Tek u slučaju posjedovanja objiju lozinki i certifikata na kartici, korisnik je autentificiran u sustav.

6.3.2. KRIPTOVALUTE - BITCOIN

Upotreba kriptovaluta, odnosno u ovom primjeru Bitcoina, primjer je korištenja kriptografije s javnim ključem. Javni ključ Bitcoinu služi kao funkcija iz koje računa adresu na koju šaljemo neki iznos, odnosno koristimo javni ključ osobe kojoj šaljemo sredstva, jednako kao što se kod kripografije služimo njime da nekome pošaljemo poruku. Privatnim, tajnim ključem, odobravamo transakciju sa svoga računa. Privatni ključ je 256-bitni broj, odnosno postoji oko 10^{77} brojeva mogućih ključeva.

Kao i svaki bitan podatak, privatni ključ treba držati minimalno na dvama mjestima (preporuka na tri), te paziti da se ne izgubi. Svatko tko posjeduje naš privatni ključ, može obaviti transakciju u naše ime.

6.3.3. CRYPTOLOCKER

Jedna od vrsti *ransomwarea*, zlonamjerni računalni program, trojanac, napravljan s ciljem „zaključavanja", odnosno kriptiranja korisničkih dokumenata te traženja otkupnine za njih. Budući da on nije virus, većina antivirusnih programa neće ga detektirati. Program koristi asimetričnu kriptografiju, odnosno šifriranje pomoću javnog i dešifriranje pomoću tajnog ključa. Ovisno o verziji, koristi različite algoritme, pa čak i 2048 bitni RSA ključ. Javni ključ pohranjuje se na napadnutom računalu i pomoću njega provodise šifriranje, dok se tajni ključ (za dešifriranje) pohranjuje na nekom udaljenom serveru pod kontrolom napadača.

Nakon završenog kriptiranja podataka, od korisnika se traži otkupnina kako bi mu se dostavio tajni ključ kojim može dekriptirati svoje podatke.

Jedini učinkovit način zaštite podataka je redovita izrada *backupa* (sigurnosne kopije), kao i kod svih drugih mogućih uzroka gubitka podataka, tako i kod *cryptolockera*. Sigurnosna kopija bi se trebala izvoditi u redovitim vremenskim intervalima (tjedan, mjesec) te spremati izvan računala, budući da neke verzije *cryptolockera* mogu zaključati i vanjske i mrežne diskove.

6.4. LITERATURA

Brown, A.C. (1975). *Bodyguard of lies*. New York, NY: Harper & Row.

Copeland, B.J. (21. siječnja 2010). *Ultra Allied Intelligence Project*. Preuzeto s https://www.britannica.com/topic/Ultra-Allied-intelligence-project, 12.7.2018.

Čavrak, H. (b.d.). ENIGMA. Preuzeto s http://e.math.hr/enigma/index.html, 12.7.2018.

Dujella, A. (b.d.). Preuzeto s http://e.math.hr/vigenere/index.html, 12.7.2018.

Dujella, A. i Maretić, M. (2007). *Kriptografija*. Sveučilište u Zagrebu: ELEMENT.

Enigma. (b.d.). U: Wikipedia. Preuzeto s https://commons.wikimedia.org/wiki/File:Bundesarchiv_Bild_101I-241-2173-09,_Russland,_Verschl%C3%BCsselungsger%C3%A4t_Enigma.jpg, 12.7.2018.

Galinović, A. (2005). *Povijest kriptografije*. Preuzeto s http://web.zpr.fer.hr/ergonomija/2005/galinovic/index.html, 12.7.2018.

Kahn, D. (1979). Šifranti protiv špijuna I-IV. (CIP Zagreb, Trans.). New York, NY: The Codebreakers (originalni članak je objavljen 1967. godine)

Ledinek, S. (26. rujna 2016). Što je Ransomware i zašto nitko nije imun? Preuzeto s http://www.pcekspert.com/clanak/sto-je-ransomware-i-zasto-nitko-nije-imun/, 12.7.2018.

Lončar, Z. (16. studenog 2017). *Kriptografija za smrtnike*. Preuzeto s https://bitfalls.com/hr/2017/11/16/cryptography-mortals-lets-explain-public-private-keys/, 12.7.2018.

University of Virginia, Department of Computer Science: Cryptology - Principles and Applications (16. rujna 2016). Preuzeto s http://www.cs.virginia.edu/cs588/challenges/jeffersonwheel/, 12.7.2018.

World Science Festival. (14. svibnja 2013). *The Enigma Machine Explained*. Preuzeto s https://www.youtube.com/watch?v=ASfAPOiq_eQ, 12.7.2018.

7. ZAKLJUČAK

Ovim *Priručnikom* željeli smo educirati prosječnog korisnika svih vrsta informacijskokomunikacijskih računalnih sustava, ali još više od toga - htjeli smo pobuditi svijest o važnosti zaštite sustava i digitalnih podataka kroz zaštitu osobne privatnosti samog korisnika.

Rezultati dosadašnjih istraživanja su ustanovili zabrinjavajuću razinu rizičnog ponašanja računalnih korisnika te su pokazali veliku potrebu za ovakvim *Priručnikom* koji će biti osnova za različite vrste edukacija, od stručnih radionica pa sve do poslijediplomske razine u vidu specijalističkih studijskih programa koji će se sustavno baviti ovom problematikom.

U prvim poglavljima *Priručnika* prezentirani su rezultati nacionalnog istraživanja rizičnog ponašanja i znanja računalnih korisnika te su istaknuta pravila za sigurno ponašanje na internetu. Neka od tih pravila su opće poznata, međutim slabo se primjenjuju.

Sljedeća poglavlja upoznaju prosječnog korisnika sa strukturom i zaštitom mreže koju administrira službena osoba, no pravila sigurnog ponašanja na lokalnoj poslovnoj mreži su slična općim pravilima ponašanja za zaštitu osobne privatnosti korisnika. Poglavlje koje opisuje postojeće zloćudne programe detaljno opisuje kako se zaštititi, na što paziti te kako povećati osobnu sigurnosti na internetu.

Zadnje poglavlje podučava prosječnog korisnika o povijesnom razvoju i osnovama kriptografije te pojašnjava kako kriptiranjem podataka sigurnije komunicirati koristeći razne informacijskokomunikacijske kanale na internetu.

Zaključujemo kako opreza nikad dosta, a neopreznost i lakovjernost na internetu kod mnogih korisnika interneta sve češće dolazi na naplatu. Doslovno na naplatu, jer sve prevare, lažna predstavljanja, krađa osobnih i drugih podataka na kraju se svode na financijski gubitak.

Internet učestalo koristi sve mlađa i mlađa populacija. Iako su se istraživanja prikazana u ovom *Priručniku* temeljila na mladima i odraslima, studije na razini Europske unije jasno pokazuju da su osnovnoškolci vrlo česti korisnici interneta, s velikom količinom vremena koju provode *online* (često i bez nadzora), a sve više su i predškolci upoznati s korištenjem interneta, najčešće putem roditeljskih pamentih telefona i tableta. Buduća istraživanja, kao i prevencija, morat će uključiti i ove najmlađe skupine računalnih korisnika, ukoliko žele postići dugoroč-

ne pozitivne učinke. Osim edukacije korisnika, koja se pokazala kao važna, ali ne i dovoljna mjera intervencije, ključna odrednica intervencijskih programa je izrada psiholoških profila različitih rizičnih korisnika računala, kako bi se mjere i strategije mogle ciljano primijeniti na određene skupine i u konačnici postići veću učinkovitost u zaštiti digitalnih podataka.

ŽELIMO VAM USPJEH U EDUKACIJI RAČUNALNIH KORISNIKA!

izv. prof. dr. sc. Tena Velki
doc. dr. sc. Krešimir Šolić

Dr. sc. Tena Velki radi kao izvanredna profesorica iz područja razvojne psihologije te kao prodekanica za znanost na Fakultetu za odgojne i obrazovne znanosti u Osijeku. Objavila je niz znanstvenih i stručnih radova kao i knjiga. Nositeljica je i voditeljica *Programa osposobljavanja pomoćnika za djecu s eškoćama u razvoju i osobe s invaliditetom* te poslijediplomskog specijalističkog studija *Inkluzivnog odgoja i obrazovanja*. Područjem informacijske sigurnosti i rizičnog ponašanja računalnih korisnika aktivno se bavi zadnjih 5 godina. Pisala je radove i držala predavanja na temu elektroničkog vršnjačkog nasilja, uloge online kompjuterskih igara u nastavi, a sudjelovala je i u organizaciji okruglog stola „Tehnologijom lakše do dječjih prava". Najznačajniji je doprinos izrada mjernog instrumenata *Upitnika znanja i rizičnog ponašanja računalnih korisnika (Velki i Šolić, 2014)*, jednog od prvih u svijetu koji ispituje ovu problematiku.

Dr. sc. Krešimir Šolić radi na Medicinskom fakultetu kao docent gdje predaje na nekoliko predmeta koje pokrivaju područje biostatistike i medicinske informatike. Istraživački rad mu je usmjeren na područje računalne i informacijske sigurnosti vezano uz privatnost i sigurnost te ponašanje korisnika ICT mreža. Do sad je objavio oko 40 tak stručnih i znanstvenih radova. Doktorsku disertaciju na temu "Model za procjenu razine sigurnosti računalnog sustava zasnovan na ontologiji i algoritmu za evidencijsko zaključivanje" branio je 2013. godine na Elektrotehničkom fakultetu Sveučilišta Josip Juraj Strossmayer u Osijeku. Završio je CCNA Cisco akademiju mrežnog administratora te ima pet godina radnog iskustva kao CARNet sistem inženjer. Aktivni je član HDMI (Hrvatskog društva za medicinsku informatiku) te HBMD (Hrvatskog biometrijskog društva).